Lecture Notes in Computer Science 1740

Rainer Baumgart (Ed.)

Secure Networking – CQRE [Secure] '99

International Exhibition and Congress
Düsseldorf, Germany, November/December 1999
Proceedings

Springer

Lecture Notes in Computer Science 1740
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Rainer Baumgart (Ed.)

Secure Networking – CQRE [Secure] '99

International Exhibition and Congress
Düsseldorf, Germany, November 30 - December 2, 1999
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Rainer Baumgart
Security Networks GmbH
Weidenauer Str. 223-225, 57076 Siegen, Germany
E-mail: baumgart@secunet.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Secure networking - CQRE (Secure) '99 : international exhibition and congress, Düsseldorf, Germany, November 30 - December 2, 1999 / Rainer Baumgart (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1740)
ISBN 3-540-66800-4

CR Subject Classification (1998): C.2, E.3, D.4.6, K.6.5

ISSN 0302-9743
ISBN 3-540-66800-4 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10749957 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The CQRE [Secure] conference provides a new international forum giving a close-up view on information security in the context of rapidly evolving economic processes. The unprecedented reliance on computer technology has transformed the previous technical side-issue "information security" to a management problem requiring decisions of strategic importance. Thus one of the main goals of the conference is to provide a platform for both technical specialists as well as decision makers from government, industry, commercial, and academic communities. The target of CQRE is to promote and stimulate dialogue between managers and experts, which seems to be necessary for providing secure information systems in the next millennium.

Therefore CQRE consists of two parts: Part I mainly focuses on strategic issues of information security, while the focus of Part II is more technical in nature. This volume of the conference proceedings consists of the reviewed and invited contributions of the second part.

The program committee considered 46 papers and selected only 15 for full presentation. For the participants' convenience we have also included the notes of the invited lectures and short workshop talks in this volume.

The selection of papers was a difficult and challenging task. I wish to thank the program committee members who indeed did an excellent job in reviewing and selecting the papers and providing useful feedback to authors. Each submission was blindly refereed by at least three reviewers to make the selection process as fair and objective as possible. The program committee was assisted by many colleagues who reviewed submissions in their field of expertise. My thanks to all of them.

I would also like to thank the entire CQRE-team for their kind assistance in organizing this event. My special thanks to our hosts from Messe-Düsseldorf GmbH and especially to N. Mizera, M. Kotschedoff, S. Spamer, A. Viefers, and B. Wagner who greatly contributed to the success of this challenging project with their untiring engagement and timely decisions. Furthermore I would like to thank the team from Brodeur-Kohtes & Klewes around B. Boendel and my colleagues T. Gawlick, A. M. Schlesinger, and D. Hühnlein for kindly assisting me in administrative tasks.

Last but not least, I wish to thank all the authors who submitted papers, making this conference possible, and the authors of accepted papers for updating their work in a timely manner , allowing the production of these proceedings.

September 1999 Rainer Baumgart

Table of Contents

PKI-experiences (Workshop Notes)

Mobile Security

Cryptography

Network Security (Workshop Notes)

Key Recovery

Intrusion Detection

Interoperability

Biometrics

Developing Electronic Trust Policies Using a Risk Management Model

Dean Povey

Security Unit, Cooperative Research Centre for Enterprise Distributed Systems**,
Level 12, S-Block, Queensland University of Technology,
Brisbane Qld 4001, Australia,
povey@dstc.edu.au

Abstract. Trust management systems provide mechanisms which can enforce a trust policy for authorisation and web content. However, little work has been done on identifying a process by which such a policy can be developed. This paper describes a mechanism for developing trust policies using a risk management model, and relates this to a conceptual framework of trust. The process uses an extended risk management model that takes into consideration beliefs about the principals being trusted and the impersonal structures and systems involved.

The paper also applies the extended risk management model to a hypothetical case study in which an individual is making investments using an electronic trading service.

1 Introduction

Regardless of the strength or robustness of a given security mechanism, its effectiveness is limited without the existence of trust. Security protocols, cryptographic devices and digital signatures rely on the ability to trust either one or more parties, mechanisms or equipment to be sure that the assets they protect remain safe.

In the physical world we derive much of our notions of trust from the tangible nature of things. For example, we perceive the information in a book to be worth reading because we know that it costs a lot of money to print a book, because the logo on the side shows that it has been reviewed by a publisher of repute, and often because a library has thought it worthwhile enough to stick it on their shelf. Similarly, we are convinced by the stability and trustworthiness of a bank, because the difficulty of licensing a fraudulent organisation and the cost of setting up branches, ATM networks and marketing etc, would make it prohibitively expensive.

However, the shift toward e-commerce means that we can no longer infer trust from physical, tangible things. We need to rethink our approach to trust

** The work reported in this paper has been funded in part by the Co-operative Research Centre Program through the Department of Industry, Science & Tourism of the Commonwealth Government of Australia

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 1-16, 1999

so that we can rely on the information and actions of people in a virtual world, with the same degree of confidence that we do in the real world.

Trust management systems such as PolicyMaker[1], KeyNote[2], and REFEREE[3] provide mechanisms that can enforce a trust policy for authorisation and web content. However, little work has been done on identifying a process by which a trust policy for such systems can be developed.

This paper describes a mechanism for developing trust policies using a risk management model, and outlines a hypothetical case study to illustrate the usefulness of such a scheme.

2 Risk Management

Risk management is the total process of identifying, controlling, and minimising the impact of uncertain events [4]. The Common Criteria [5] outlines a model for relating different elements of the risk management process, which is given in figure 1. In general, risk management for information security involves the following process:

1. Identify the assets to be protected, the threats to these assets, and the expected impact if those assets are compromised.
2. Identify the vulnerabilities or weaknesses which can lead to these threats arising.
3. Analyse the risk (i.e. the likelihood and consequences) of the vulnerabilities leading to these threats being exploited.
4. Determine whether to accept or treat the risk.

Risk is treated using countermeasures which seek to reduce either the likelihood or consequence of a risk, or defer the risk to some third-party (e.g. insurance). Implementing a countermeasure has a cost associated with it, which must be balanced against the expected utility of implementing the measure. Countermeasures may also expose additional risks, or retain residual risk which must be considered in the risk management process.

Risk management is well understood, and numerous standards and methodologies exist to describe the process (e.g. [6][7][8]). Integrating risk management into the trust management process is therefore useful, as it will enable us to leverage off this existing body of work.

3 Trust

To integrate trust with risk management, it is necessary to provide a framework by which different aspects of trust can be described and related. One of the more comprehensive frameworks for trust was developed by McKnight, Cummings and Chervany, and results from a survey of sixty papers across a wide range of disciplines[9][10]. McKnight et al's model provides a classification system for different aspects of trust, as well as a system for showing how trust can influence behaviour and defines the following constructs:

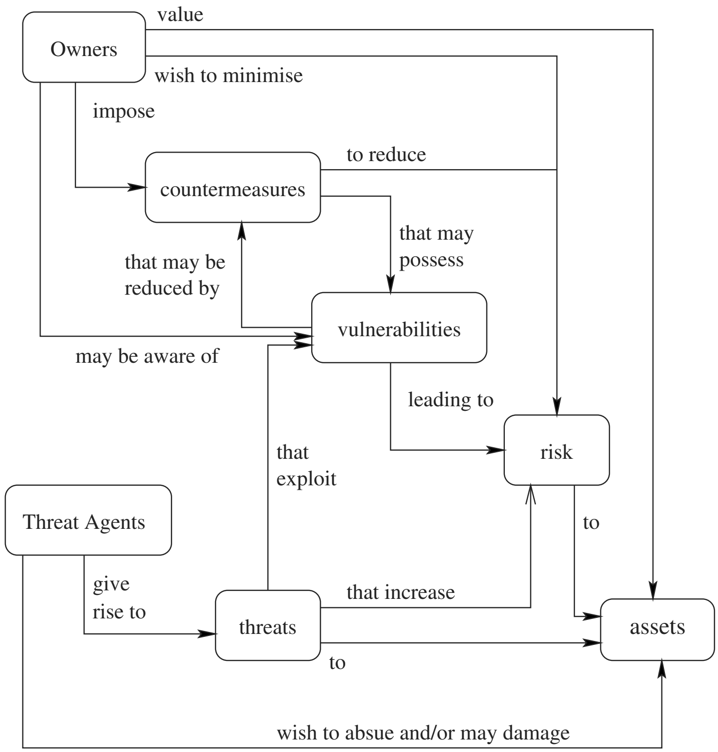


Fig. 1. Security concepts and relationships from the Common Criteria

Trusting behaviour the extent to which one person voluntarily depends on another person in a specific situation with a feeling of relative security, even though negative consequences are possible. This construct is in effect describing the "act" of trusting, and implies acceptance of risk (negative consequences) by the trusting party.

Trusting intention the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible. A trusting intention usually leads to trusting behaviour. Trusting intentions relate directly to the security policy which determines how entities in the system are trusted. A trusting intention essentially specifies a willingness to trust a given individual in a given context, and implies that the trusting entity has made decisions about the various risks and benefits of allowing this trust.

Trusting beliefs the extent to which one believes and feels confident in believing that the other person is willing and able to act in the trusting party's best interests. A trusting intention will be largely based on the trusting par-

ties cognitive beliefs about the other person. McKnight et al describe four categories of trust belief:

1. Benevolence - the belief that a person cares about the welfare of the other person;
2. Honesty - the belief that a person makes agreements in good faith;
3. Competence - the belief that a person has the ability to perform a particular task; and
4. Predictability - the belief that a person's actions are consistent enough to forecast what they will do in a given situation.

Trusting beliefs characterise the information by which we make our trusting decision about a given individual. They may be based on evidence, recommendations from third parties (which themselves must be trusted), and often by simple intuition. We can think of trusting beliefs as being the measures by which we will determine whether a given entity should be trusted given a specific risk profile. It should be noted that not all beliefs need to be strong in order to trust an individual in a given context. In business transactions, the issue of benevolence is rarely important (although the presence of malevolence may be) when compared to the issues of honesty, predictability, and most importantly competence. Also, some beliefs are easier to be confident about than others. It is usually simpler to obtain a measure of an organisations competence (by accreditation and recommendations), and predictability (by past dealings); than it is to obtain a measure of their benevolence and honesty.

Like trusting intentions beliefs may also be specific to a context (e.g. belief in the competence of a lawyer to write contracts, does not extend to their competence to perform neurosurgery).

As we shall see it is trusting beliefs which are the most important to ascertain, as they will determine the confidence by which we establish our trusting intentions.

System trust the extent to which one believes that proper impersonal or institutional structures are in place to enable one to anticipate a successful future endeavour. An important difference between system trust and trusting beliefs, is that while trusting beliefs relate to the attributes of another person whom is being trusted, system trust relates to the actual system/infrastructure under which the trusted action is taking place.

System trust is important, as it provides stability to our interactions with people and organisations. Legal and regulatory systems provide punitive mechanisms to discourage malicious behaviour, and accreditation and certification schemes provide systems which allow us to evaluate an organisations competence. Like trusting beliefs, system trust is a critical component of determining a trusting intention.

Dispositional trust the extent to which one has a consistent tendency to trust across a broad spectrum of situations and persons. A person may have dispositional trust because they either believe in the general good nature of people, or they believe that they will achieve better outcomes by tending to trust people.

Situational trust the extent to which one intends to depend on a non-specific party in a given situation. Situational trust is related to dispositional trust in that it is a general intention. However, it is differentiated by the fact that where dispositional trust refers to a broad spectrum of situations and persons, situational trust is related only to a specific situation.

Belief formation processes The process by which new beliefs are developed and integrated into our schema about the world.

These constructs do not exist in isolation, but have well-defined relationships between them. We can clearly see that a trusting behaviour relies on the existence of a trusting intention, which in turn is created through the existence of one or more of trusting beliefs, system, dispositional or situational trust. Figure 2 shows the various constructs and their dependencies.

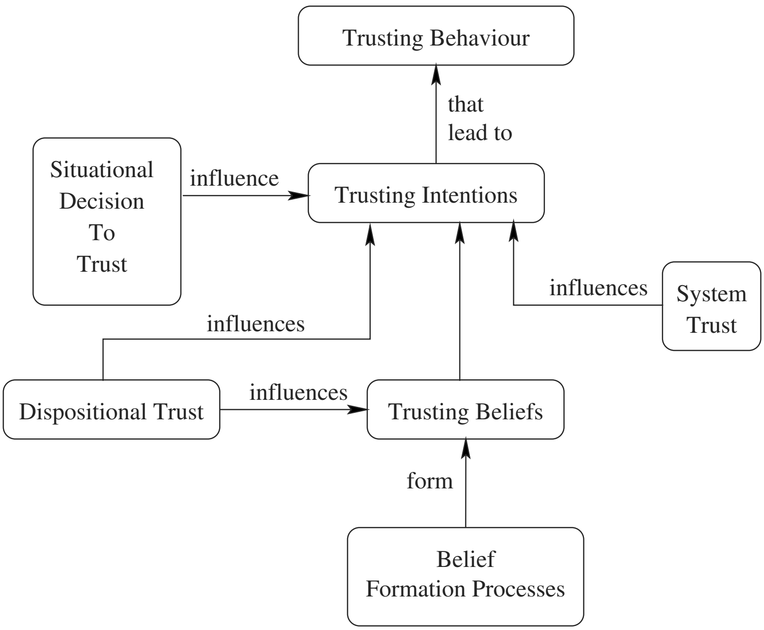


Fig. 2. Related Trust Constructs

McKnight et al's conceptualisation of trust as multi-dimensional is both powerful and compelling. It also goes some way to explaining the difficulty that researchers in many disciplines have encountered in the formulation of a single broad definition of what trust is. In addition, their wide consultation of literature from many disciplines including management, communication, sociology, social psychology and economics, positions their model within a context that it is sufficiently broad to categorise most definitions of trust.

4 An Extended Risk Model

To extend the risk model to encompass trust, it is important to see the goal we are trying to achieve in developing a trust policy. A risk management process seeks to identify risks, and to determine whether those risks should be treated or accepted. Trust management on the other hand, seeks to identify the circumstances under which we are prepared to accept risks that may be exposed by relying on certain entities. The key to merging these two concepts is to focus on risk as the common element. We can see that the definition for trust management can be related to the decision about risk acceptance/treatment. In effect, trust becomes a risk treatment option, i.e. you are prepared to accept risks if you trust the entities that can expose them.

This fact is intuitively obvious to most people. The more someone is trusted, the more we feel we can rely on them, and consequently the more risk we expose ourselves to. When we talk about levels of trust, we are really discussing the level of risk that we are prepared to accept for relying on a trusted entity.

4.1 Relating Trust Policies to McKnight et al's Model

The constructs described in section 3 provide a vocabulary for describing how trust is formed. By combining this process with the risk management process we can show how trust policies can be captured from the environment using a structured process.

In McKnight et al's model, the trusting intentions form the trust policy, which is essentially a statement of the conditions under which we are prepared to trust a given entity. As noted in section 3, these intentions are formed from a number of sources: our dispositional trust, our beliefs about the entity we are trusting, how we trust the systems which we look to to support and protect us, and our tendency to trust in the given situation. As described, it is important to consider the risks of the behaviour of entities that we intend to trust. However, it is also important to consider the utility or value of trusting this entity, as this can considerably alter the decision to accept or treat a risk, or to not allow the behaviour to occur.

On further analysis, we see that there is also important interactions between components of the trust framework that we must consider. One of the most important elements of forming the trusting intention is the existence of trusting beliefs about an entity. These are important, as they are the only input into the trusting intention decision which is specific to a given entity. McKnight et al's model identifies a *belief formation process*, which is an iterative mechanism that uses information and experience gathered from the environment to form one or more trusting belief about an individual. In this extended risk management model, the information that is input into this process is called a *trust metric*. Trust metrics contribute to our understanding about the four trusting beliefs (competence, predictability, honesty and benevolence); and include:

- information based on previous experience;

- recommendations from third parties;
- certifications or qualifications;
- memberships of professional organisations;
- certified histories (criminal records, credit reports etc.); and
- brand.

As we can see from this list, the trust metrics themselves can be subject to trust decisions about their accuracy. Thus, the belief formation process is recursive.

Another important observation, is that metrics may have a cost associated with them (e.g. obtaining a credit report may cost money). In developing a trust policy, we must be careful to ensure that the costs of gathering metrics do not outweigh the utility gained from trusting, and that we maximise the value of our metrics, such that the cost reflects the contribution to our understanding of the trusting beliefs.

Figure 3 shows how these constructs relate to form an extended risk model.

4.2 Using the Extended Risk Model for Trust Management

By combining the concepts from risk management with the extended risk model, we can establish the following process for establishing a trust policy:

1. Identify the entities and situations you want to determine a trust policy for. This allows the establishment of *trust contexts*, which encapsulate the security context within which trust decisions will be made. Note that such a context should include both all probable trusted entities and threat agents.
2. Identify the assets to be protected within this trust management context, the threats to these assets, and the expected impact if those assets are compromised.
3. Calculate the expected utility of trusting entities in the given situations.
4. Identify the vulnerabilities or weaknesses which can lead to these threats arising.
5. Analyse the risk (i.e. the likelihood and consequences) of the vulnerabilities leading to these threats being exploited.
6. Determine the adequacy of existing countermeasures which may mitigate these risks.
7. Determine the required beliefs and confidences in these beliefs required to trust (or distrust) entities which may expose the given risks.
8. Identify the various impersonal structures or systems which have an impact on the given trust context. Common systems will include legal or regulatory frameworks. Analyse our confidence in these systems to mitigate risks.
9. Identify metrics which will can help make decisions about the required trusting beliefs, and determine the confidence we have in the accuracy of these metrics (in itself a mini trust-management decision).
10. Evaluate the costs of gathering these metrics, and relate this to the expected utility, and their contribution to confidence in the trusting beliefs. Use this evaluation to select the subset of metrics which can be used to establish the trusting beliefs.

11. Using the metrics, establish the beliefs identified in step 7 and determine whether they meet the required confidence levels.
12. Based on this evidence and the levels of system trust, either unconditionally accept a trusting intention for the evaluated entity in the given situation; reject the trusting intention; or treat the risk and reevaluate.

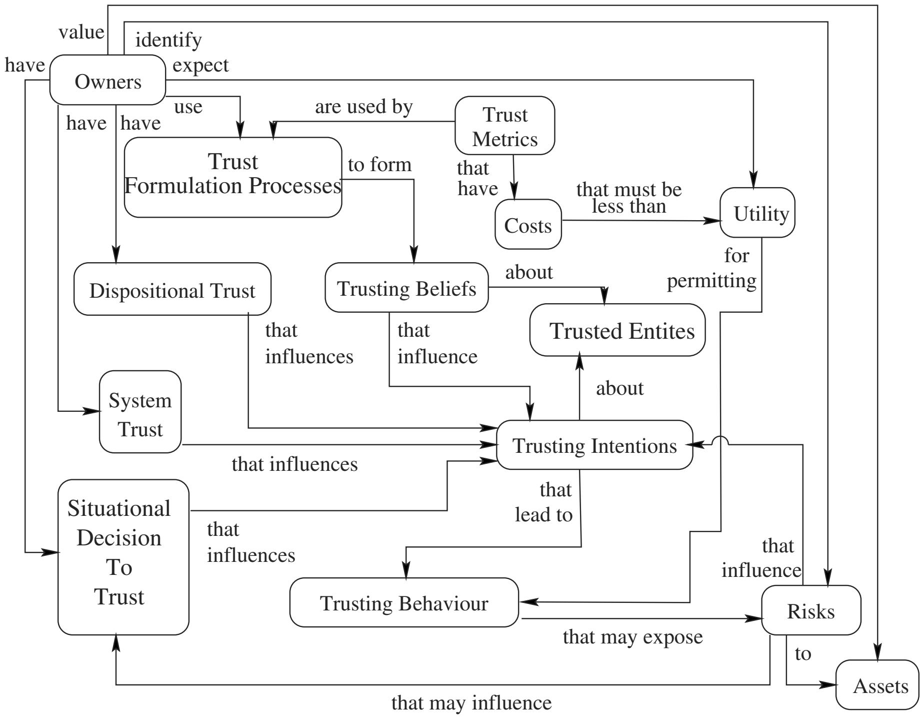


Fig. 3. Extended Risk Model

Trusted entities and threat agents may be either known or unknown. In the case that they are known, then the policy should include the actual measurements for this entity obtained using the trust metrics. In the case that they are unknown, the policy should contain the list of metrics which are required to determine whether an entity should or should not be trusted.

If a trusting intention is rejected, then risk may be treated by a number of mechanisms:

1. Add countermeasures which decrease the risk
2. Defer risk to a third party (e.g. insurance)
3. Increase the required belief trusting confidences by obtaining more or better metrics.

We can see that this process extends the risk management by integrating components of the trust model.

5 Writing Trust Policies

The outcome of the trust management process should be a policy which documents the decisions made. The policy should include:

Trust metrics A list of the metrics used in a trust policy, the trusting beliefs they measure, and their appropriateness for given trust contexts.

Confidence levels A description of the list of qualitative or quanti tative labels that indicate our level of confidence in a given trusting belief.

Trust context policies An articulation of the policy for making trusting decisions for each of the identified trust contexts.

These items are described below.

5.1 Trust Metrics

One important component of the extended risk model is the use of trust metrics. These are mechanisms which can be used to enhance our confidence about certain beliefs. An important thing to note is that the trust metrics themselves need to be trusted, and we will have a confidence level associated with their precision. A trust policy should begin by evaluating the trust metrics which it will use, and providing confidence levels which we have in their measurements in a given context.

When specifying the metrics used in the policy, the policy writer should state:

- the contexts in which that metric is trusted;
- the belief(s) that they measure;
- the confidence in that metric for those contexts in which it is trusted, and how this is measured (NB: metrics can be evaluated using other metrics); and
- the cost of evaluating that metric.

In general, metrics should require close scrutiny as we are exposed to more systemic risk by trusting them.

5.2 Confidence Labels

The policy writer should include confidence labels which may be attached to particular beliefs in the trusting decision. Confidence labels can be either qualitative or quantitative, and are similar to the likelihood measurements which are commonly used in risk management. The confidence label represents the likelihood that the belief it is attached to is correct, i.e high confidence means a high probability of correctness. Figure 4 gives an example of qualitative and

Label	Quantitative	Qualitative
Very Low	A belief with this label has very low confidence, it should only be relied on if the risk is negligible.	$p <= 0.5$
Low	A belief with this label has low confidence, it may be relied on only if the risk is low.	$p > 0.5$
Medium	A belief with this label has medium confidence, it may be relied on for contexts at medium risk	$p > 0.95$
High	A belief with this label has high confidence, it may be relied on in high risk situations.	$p > 0.995$
Very High	A belief with this label has very high confidence, it may be relied on in all situations.	$p > 0.999$

Fig. 4. Example confidence labels

quantitative labels which might be used in a trust policy. In the quantitative descriptions, p is the probability that a belief with that given label is correct.

Confidence levels may be combined to obtain new confidence measures. This is useful when for example a number of metrics are being used to determine the level of a trusting belief. Quantitative metrics can be combined, simply by summing the probabilities (i.e. only one of the metrics has to be correct, for the belief to be correct). Qualitative metrics can be combined either on an ad hoc basis or by using rules to combine levels (e.g. HIGH = 3 $\times$ MEDIUM).

5.3 Trust Contexts

These are all the situations and environments that are under consideration for the trust policy. For each trust context, the trust policy should detail:

- a description of the context;
- the risks inherent in trusting entities for a given context;
- the expected utility of trusting entities for the given context;
- a list of the possible trusted and threat agents;
- a list of the beliefs and confidences required to trust/distrust entities in the trust context; and
- a list of the required/available metrics appropriate to establish these beliefs.

Contexts may be included within other contexts, for example a context which covers user access to a web site, may also include a sub-context for privileged access to files. This allows a simple hierarchical organisation of trust policies.

If specific entities are to be trusted for a given context, these entities should be listed along with the rationale for trusting them. Where the policy is specifying criteria for trusting unknown entities, it is sometimes useful to separate out the requirements in terms of the type of entity which is to be trusted. For example, entities could be divided into customers, employees and contractors. The policy writer may wish to express differing levels of required beliefs and confidences in each of these, as there are varying levels of utility for differing classes to exploit threats, and as such varying likelihood of threats occurring.

6 Hypothetical Case Study

In this section, the extended risk management model is applied to a hypothetical case study in which an individual is making investments using an electronic trading service. The case study serves to illustrate the complexity involved in evaluating a given trust decision, as it shows how making one trust decision relies on many other trust decisions. It should be noted that in the following example, some of the steps described in section 4.2 have been consolidated together. The aim is to give a general feel to how a trust policy can be developed using the mechanism, and not to explicitly show how the policy should be expressed.

6.1 Scenario

Bob is a naïve investor, with a small amount of cash to spend. He is contemplating some direct share investments, and so asks his friend Alice who is wise in the ways of sharemarket for her advice. Alice suggests he makes a number of investments, but recommends in particular, a recently listed small Internet company – ComDot.com. She says that she has heard on the grapevine, that this company is likely to do spectacularly well, once it releases the next version of its new Website construction software. Alice also suggests that rather than fork out for brokerage fees, Bob purchase the shares directly from E-Shares, an online brokering firm which allows small purchases using a credit card. Bob contemplates whether to take Alice's advice.

6.2 Trust Management Process

Based on the information from Alice, Bob has to make a number of decisions about whether to invest in ComDot.com shares. Doing this requires a number of trusting decisions, which may also involve gathering information, and determining whether that should be trusted. Following the trust management process outlined in section 4.2, Bob sets about determining his trust policy.

Establishing Trust Management Context The scenario above constitutes Bob's trust management context, i.e. he is making decisions about trust within the context of making a specific decision about buying a certain set of shares using an electronic trading service. There are a number of trusting intentions which Bob must have before he can make this decision:

1. Bob must trust Alice to give good advice about the shares;
2. Bob must trust ComDot.com to conduct their business competently; and
3. Bob must trust E-Shares to respect his privacy, and keep his credit card details secure.

In addition, Bob must also consider threats from the following sources:

– hackers, who wish to steal Bob's credit card details and make fraudulent purchases;

– ComDot.com's competitors who may wish to spread misinformation in order to gain market advantage; and
– marketeers, who may wish to use knowledge of Bob's share purchase as fuel for direct marketing campaigns.

Calculate Expected Utility By purchasing the shares, Bob aims to make at least an 8% per annum return on his investment. By using the online trading scheme he hopes to save up to 20% in brokerage fees.

Identify Assets to be Protected In this scenario, Bob determines that he has three main assets under threat:

1. The cash he is investing (could be lost due to poor investment)
2. His credit card number (there is a threat of disclosure leading to fraudulent transactions on his credit card).
3. His privacy (Bob doesn't want people knowing how he spends his money).

Vulnerability Analysis By analysing his assets and the possible threats, Bob determines the set of vulnerabilities which may lead to those threats being realised.

1. Information Bob uses to make decisions could be inaccurate.
2. Companies which Bob invests in might go out of business
3. E-shares might disclose private information
4. E-shares might disclose Bob's credit card details
5. Hackers might intercept Bob's credit card details over the Internet.

Risk Analysis For each of the above vulnerabilities, Bob identifies the likelihood and consequences of these vulnerabilities causing threats to be realised. Likelihood is measured qualitatively (RARE, UNLIKELY, MODERATE, LIKELY, CERTAIN), and the label UNKNOWN is used where making this judgement is not possible in this first analysis (usually due to lack of knowledge about trust levels). Consequences are also indicated qualitatively with the labels: INSIGNIFICANT, LOW, MODERATE, SIGNIFICANT, CATASTROPHIC). This analysis is summarised in figure 5.

Identify Required Beliefs and Confidences Bob now needs to determine the level of required beliefs in order to accept the risks he has identified. We shall briefly outline these decisions for two of the identified vulnerabilities:

Information Bob uses to make decisions could be inaccurate Given the risk identified, Bob determines that he has to trust the information he receives about given shares with a HIGH degree of confidence (see figure 4). In order to trust the information he receives, Bob determines he has to know that the sources of the information are competent, honest and predictable; and that his confidence in these beliefs must either be HIGH, or the information must be confirmed from other sources, such that the total confidence for each of these beliefs is HIGH.

Item #	Likelihood	Consequences	Comments
1.	UNKNOWN	SIGNIFICANT	Likelihood depends on how much we trust the source of information
2.	MODERATE	SIGNIFICANT	–
3.	MODERATE	SIGNIFICANT	–
4.	MODERATE	LOW	Low consequences, as vendor bares liability for all but \$50 of fraudulent transactions
5.	UNLIKELY	LOW	As above, but SSL encrypted link which makes it less likely.

Fig. 5. Risk analysis Summary

E-shares might disclose Bob's credit card details Given the identified level of risk, Bob decides he needs to only have MODERATE confidence in E-shares competence to protect his credit card details.

Identify and Evaluate Metrics When relying on information or actions, Bob determines the following metrics to be used to determine the confidence he has in certain beliefs about that entity.

– previous experience with the entity (MEDIUM-HIGH confidence);
– recommendations from other trusted sources (MEDIUM confidence);
– established brands (MEDIUM confidence);
– contractual obligations (HIGH confidence); and
– regulatory controls (MEDIUM confidence).

In addition, he determines the following additional metrics to be used where specific software countermeasures (e.g. the SSL enabled browser he uses) are used to combat risk:

– ITSEC or Common Criteria evaluation (HIGH);
– open source software which has been heavily scrutinised (MEDIUM);
– well known product or vendor (MEDIUM); and
– recommendations from other trusted sources (LOW-MEDIUM).

Lastly, Bob determines the following metrics which are used where he is relying on a third party security system.

– disclosure of security practices and procedures (LOW);
– third party audit by a trusted auditor (MEDIUM-HIGH); and
– certified quality system (e.g. ISO9000) (MEDIUM-HIGH).

Belief Analysis

Information Bob uses to make decisions could be inaccurate Bob has already determined the following beliefs about two entities he will rely on for information:

– Alice: Competence (MEDIUM), Honesty (HIGH), and Predictability (HIGH). Alice can be trusted for information, providing the information is confirmed from at least one other mediumly trusted source. These beliefs were determined solely from a long history of past experience with Alice.
– Reuters News-Wire service: Competence (MEDIUM-HIGH), Honesty (HIGH), and Predictability (HIGH). Reuters can be trusted to report information, providing it can be confirmed by at least one other LOW-MEDIUM trusted source. These beliefs are determined by Reuter's good brand, recommendations from Alice and other friends, and previous experience.

E-shares might disclose Bob's credit card details Bob determines a HIGH level of confidence about E-shares' competence to keep his credit card details secure. This belief is determined from the existence of a certified ISO9000 quality system and a third party audit from KPMG which E-shares describe on their web sites.

Trusting Decisions Figure 6 summarises Bob's trusting decisions for each of the identified vulnerabilities.

Item #	Trust decision	Comments
1.	Accept Risk	Trust Alice's information (confirmed by a Reuter's article), and a policy is described for trusting subsequent information
2.	Accept Risk	Sufficient information is available to trust ComDot-.com's competence to do well. A policy is described for obtaining the required trust in other companies whose shares Bob wants to purchase.
3.	Accept Risk	Bob determines E-shares' privacy policy is sufficient, and trusts them to enforce it.
4.	Accept Risk	Bob is convinced by third party evidence that E-shares' is competent at keeping its site secure enough to mitigate this risk.
5.	Accept Risk	Bob trusts the SSL mechanism used to secure communications with E-shares, and trusts his browser and E-shares web server to implement this mechanism correctly.

Fig. 6. Trusting decisions summary

6.3 Summary

This hypothetical case study outlines the application of the trust management process based on the extended risk model. It should be noted that only a sub-

section of the full analysis is presented. Nevertheless it serves to illustrate the plausibility of such a technique in a real world situation.

7 Related Work

Khare and Rifkin [11] describe how trust management philosophies can be applied to the World Wide Web, and describe how trust policies can be designed. However, Khare and Rifkin's work is very much focused on the expression of trusting intentions, i.e. they describe how to express a trust policy, but do not provide a methodology for how to derive it.

In [12] Jøsang describes general criteria for modelling trust in information security and critiques some other existing formal schemes. Further work by Jøsang [13] develops these ideas into a formal model based on a concept called *subjective logic*. Subjective logic allows us to reason about beliefs or opinion using an algebraic notation, and would be useful in the context of working with trusting beliefs in the extended risk model.

As indicated, there have been several attempts to build trust management systems [1][2][3]. Of these REFEREE[3] is probably the most notable, as it provides way to integrate with third party recommender systems like the PICS [14] labelling scheme. The REFEREE architecture is also extensible, making it simple to integrate new components into the system. Future work on automating the trust management process could benefit highly by utilising REFEREE as a platform for gathering and evaluating information.

8 Future Work

Decision support systems is a catch all for a wide variety of systems which provide computer support for decision making [4]. There is a significant body of work on using decision support systems for risk management [15][8], which could be leveraged to develop similar systems for trust management based on the extended risk model.

Another direction for this work might be the development of trust metrics which could be used to automatically establish beliefs about pages on the World Wide Web. Examples of such metrics might include:

- number of pages linking to a given web page;
- trusted pages linking to given web pages;
- third party recommendations (e.g. PICS labels); and
- number of hits on a given web page.

Search engines might be useful sources for such information. In particular the Google search engine [16] already uses link counts in order to rate matched pages.

Lastly, the importance of considering dynamically changing policies needs to be investigated. Beliefs and trust are not static, but change as new information is received. It would be useful to investigate how policies could be defined which cope with dynamic changes.

9 Conclusions

This paper has presented a scheme for developing trust policies based on an extended risk management model. The scheme was applied to a hypothetical case study, which shows the utility of the process to real world applications. The paper has also discussed related work and given some firm directions for future research in this area.

References

1. M. Blaze, J. Feigenbaum, and J. Lacey. Decentralized trust managment. In *Proceedings of the 1996 Symposium on Security and Privacy*, pages 164–173, 1996.
2. Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. Keynote: Trust managment for public-key infrastructures. In *Cambridge 1998 Security Protocols International Workshop*, England, 1998.
3. Yang-Hua Chu, Joan Feigenbaum, Brian LaMacchia, Paul Resnick, and Martin Strauss. Referee: Trust management for web applications. In *Proceedings of the 6th International WWW Conference*, 1997.
4. Dennis Longley, Michael Shain, and William Caelli. *Information Security: Dictionary of Concepts, Standards and Terms*. Macmillan, 1992.
5. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, May 1998.
6. Standards Australia/Standards New Zealand. AS/NZS 4360:1999 Risk Management, 1999.
7. Communications Security Establishment (CSE) Government of Canada. A guide to Security Risk Managment for Information Technology Systems MG-2, 1992. URL: http://www.cse.dnd.ca/cse/english/Manuals/mg2int-e.htm.
8. Dennis Longley, Michael Shain, and William Caelli. *Information Security: Dictionary of Concepts, Standards and Terms*, pages 450–453. Macmillan, 1992.
9. D. Harrison McKnight, Larry L. Cummings, and Norman L. Chervany. Trust formation in new organizational relationships. In *Information and Decision Sciences Workshop*, October 1995. URL: http://www.misrc.umn.edu/wpaper/wp96-01.htm.
10. D. Harrison McKnight and Norman L. Chervany. The meanings of trust. Technical report, MISRC Working Papers Series, 1996. URL: http://www.misrc.umn.edu/-wpaper/wp96-04.htm.
11. Rohit Khare and Adam Rifkin. Weaving a web of trust. *World Wide Web Journal*, 2(3), 1997.
12. Audun Jøsang. Prospectives for modelling trust in information security. In Vijay Varadharajan, editor, *Proceedings of the 1997 Australasian Conference on Information Security and Privacy*. Springer-Verlag, 1997.
13. Audun Jøsang. A model for trust in security systems. In *Proceedings of the Second Nordic Workshop on Secure Computer Systems*, 1997.
14. W3C. Platform for Internet Content Selection (PICS) technical specification. URL: http://www.w3.org/PICS/.
15. Giampiero E.G. Beroggi and William A. Wallace, editors. *Computer supported risk management*. Kluwer Academic Publishers, 1995.
16. Google Inc. Why use Google?, 1999. URL: http://www.google.com/why_use.html.

SECURE: A Simulation Tool for PKI Design

L. Romano[1], A. Mazzeo[2], N. Mazzocca[2]

[1] Università degli Studi di Napoli "Federico II"
Via Diocleziano, 328
I-80124 Napoli, Italy
[lrom@unina.it]
[2] II Università degli Studi di Napoli
Via Roma, 29
I-81031 Aversa (CE), Italy
[mazzeo, n.mazzocca@unina.it]

Abstract. This work presents a novel methodology for security analysis of computer systems. The suggested approach, called *simulated hazard injection*, is a variant of simulated fault injection, which has already been employed with success to the design and evaluation of fault-tolerant computer systems. The paper describes the key ideas underlying the proposed methodology, and defines a portfolio of security measures to be extracted from experimental data. These concepts are incorporated in a tool for dependability analysis of Public Key Infrastructure (PKI) based systems. The tool is called SECURE and is currently under development at the University of Naples. The paper describes the architecture of the tool and discusses its potentialities.

1 Introduction

Security is of crucial importance in all automated, business-related transactions. Forms of electronic commerce, such as communication via electronic mail, Electronic Data Interchange (EDI), or the World Wide Web, are just a few examples of crucial fields of application, where a security breach may have significant economic impact and/or legal consequences. The deployment of paperless mechanisms can be highly beneficial in reducing business costs and in creating opportunities for new and/or improved customer services. However, the electronic systems and infrastructures that support electronic transactions are susceptible to abuse, misuse, and failure in many ways. All participants, i.e. commercial traders, financial institutions, service providers, and consumers are exposed to a variety of potential damages, which are often referred to as electronic risks [1]. These may include direct financial loss resulting from fraud, theft of valuable confidential information, loss of business opportunity through disruption of service, unauthorized use of resources, loss of customer confidence or respect, and costs resulting from uncertainty. In order to mitigate risks and promulgate the deployment of information security technology on a wide scale in the commercial environment, appropriate security countermeasures, and business and legal frameworks must be established. The following services must be provided [2]:

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 17-29, 1999

- Confidentiality – Provides privacy for messages and stored data by hiding information using encryption techniques;
- Message Integrity – Provides assurance to all parties that a message remains unchanged from the time it was created to the time it was opened by the recipient;
- Non-repudiation – Can provide a way to prove that a document came from someone even if he/she tries to deny it;
- Authentication – Provides two services. The first is to identify the origin of a message and provide some assurance that it is authentic. The second is to verify the identity of a person logging onto a system and after doing so, continuing to verify that person's identity in case someone tries to break into the connection and masquerade as the user.

For the most part, these services are enabled through public key (asymmetric) schemes rather than private (symmetric) schemes, for these are best able to cope with scalability problems. The distribution of keys, however, is difficult even in the public scheme if the Internet is the communication channel. On the Internet, obtaining a public key requires a certain level of trust. One must know that the public key belongs to the person one thinks it does. Someone might be masquerading as someone else. A solution is to work with a trusted third-party organization called Certificate Authority that distributes public keys for people and organizations and that verifies the credentials of the people associated with the public keys. In this way trust is transferred from a people-trusting-people to a people-trusting-an-organization scheme. This leads to a more complex organism (eventually to a world-wide global organism) incorporating independent certification authorities that can transfer trust among themselves. Such an organism is called a Public Key Infrastructure (PKI). As it is evident from the above description, a Public Key Infrastructure (PKI) is a complex organization, consisting of policies, services, and professionals. In this context, a party who acts or is in a position to act in reliance upon a certificate and its subject public key is referred to as a Certificate User or Relying Party. A certificate will become a sort of global passport and a personal database that holds a wealth of information about the certificate subject in a very secure way.
In order to make public-key-based technologies usable on a wide scale, PKIs must support a variety of services, such as:

- Registering users – This also entails authenticating certificate applicants. This task can be performed either by the Certification Authorities (CAs) or by separate entities, called Registration Authorities (RAs), that front-end Certification Authority service;
- Issuing certificates – A CA has to issue certificates to Subscribers, i.e. parties who are the subject of a certificate and who are capable of using, and are authorized to use, the private key that correspond to the public key listed in the certificate;
- Providing Information about Certificate Status – Certificates and other relevant information about certificates must be delivered or made accessible online to Certificate Users;
- Issuing Certificate Revocation Lists - If a certificate is to be revoked, Certificate Authorities needs to make potential users of the certificate aware of the revocation.

Such services must be provided in accordance to a set of well defined policies and enforced rules. These must be clearly stated in a document (or a set of documents) called Certification Practice Statement (CPS).

2 Issues

From the technological perspective, there are no major outstanding challenges. The field of information security has been studied for many years by governments, academia, and a small industry sector of specialists, and solutions to most of the technical problems are well-understood by the technology specialists. Until recently, however, these information security solutions have received little use, except for national security and certain internal banking purposes. Therefore, there is still a tremendous amount to be learned about deploying information security technology on a wide scale. In addition, diverse legal and business practices and controls must be addressed in conjunction with the deployment of technological security countermeasures. When trying to enforce security in this context, involving highly diverse organizations and communities which need to work together in complex ways, many interesting and subtle issues arise, of both a technical and a legal nature. A variety of products exist from many different vendors, which provide the mechanisms needed to build PKI based systems. None of them, however, incorporates the means to assist the system designer in identifying the optimal solution for a specific scenario. This may involve choosing between different potential architectures, and setting the most appropriate values for crucial configuration parameters, in order to maximize interoperability, while minimizing the risk and the impact of a security compromise. Increased security requirements have created an urging need for methodologies, models, and automated, cost-effective design and validation tools for trusted computer systems and infrastructures. The success of the engineering process will rely on the capability of the designers to measure or evaluate the security of each component, as well as of the overall architecture. Thus, security prediction, and evaluation must become an integral part of the system design activity. Predicting, at design time, the security level a system will achieve at operation time, is quite an hard task. Design methodologies, and tools must be provided, which allow the developer to address issues, such as: ways to structure relationships between multiple certification authorities, to associate different certification policies or practices with different certification paths, to find and validate certification paths, to develop and test certificate management protocols, and to enact legislation regarding PKIs to support digital signatures on commercial and governmental business transactions. To be efficient, the analysis must be conducted under realistic operational conditions, which take into account intentional and unintentional attacks, and other exceptional conditions.

3 Approach

The approach we suggest here is based on simulation. In the design phase of complex systems, simulation is an important experimental means for evaluating a system under a variety of aspects [3]. Simulation has many advantages over analytical modeling, some of which are reported here:

- Compared to analytical modeling, simulation has the capability to model complex systems to a high degree of fidelity without being restricted to assumptions made to keep an analytical model mathematically tractable;
- Analytical modeling tools only use probabilistic models to represent the behavior of a system. In essence, the effect of an event on the system is predefined by a set of probabilities and distributions. Functional simulation tools not only use stochastic modeling, they also permit behavioral modeling - which does not require that the effect of an event be predefined - and in some cases they allow the actual software to be integrated and executed within the simulated model. If this is the case, a number of system parameters are the results of (and not inputs to) the simulation experiment. In addition to this, unlike analytical modeling, in which only a few types of distribution are commonly used for the tractability of models, the simulation method can handle any form of distribution, empirical or analytical;
- Too many factors affect the behavior of a system on the field, which cannot be easily modeled analytically.

Even with simulation, however, a number of issues arises. A fundamental issue is *simulation time explosion*. This occurs in two cases:

1. When too much detail is simulated, such as modeling processes at an extreme level of detail;
2. When the target system is already characterized by a high security level, i.e. the probabilities of experiencing security breaches is extremely low, which means simulation sessions require a very long time, in order to collect a statistically significant amount of experimental results.

Several techniques, including mixed-mode simulation [4], importance sampling [5], and hierarchical simulation [6] can be used to address the time explosion problem.

Another fundamental issue involves *workloads*. The impact of hazards on system security is workload dependent. Hence, it is important to analyze a system while it is executing representative workloads. Workloads for simulation experiments can be trace files of real applications, selected benchmarks, or synthetic programs. If the goal of the study is to assess the security level attained by the system in a well-defined operational context, a model of the real applications to be run in the target configuration should be used in the simulation. If the goal is to study hazard impact with regard to general workloads, several representative benchmarks should be selected for the simulation. If the objective is to exercise every functional unit and location, neither real applications, nor benchmarks may be appropriate. In this case, synthetic workloads may have to be designed for achieving the goal. The workload issue complicates simulation models and increases simulation time. It is essential to develop techniques to represent realistic workloads while maintaining reasonable simulation times.

With these ideas in mind, we have developed a novel methodology, and a framework for system security analysis. The technique we suggest, herein after called *simulated hazard injection*, is a variation of simulated fault injection. Simulated fault injection has been successfully employed for dependability (reliability, availability, and performability) evaluation of fault-tolerant computer systems [7]. In simulated fault injection, faults, i.e. pathological events which may originate failures, are injected to a simulated model of the system, in order to evaluate the capability of the system to cope with errors. Simulated hazard injection consists in simulating the behavior of the target system while hazards, i.e. attacks to system security which may originate security compromises, are injected to its components, in order to evaluate the security level attained by the system. To the best of our knowledge, such an approach has never been proposed in the literature before. The following definitions are used:

- Security *hazard* – An unintentional or intentional attack to system security, which makes the system exposed to potential security breaches;
- Security *compromise* – A security breach which manifests in the system. It is the consequence of a security hazard.

Simulated hazard injection can be used to pick out the key features, define the structure, and specify the configuration parameters of the target system.

4 Measures

In order to evaluate the security level of the system, quantitative measures must be defined and support must be made available to extract such measures from experimental data.
Based on the previously defined concepts of hazard and compromise, we have identified a portfolio of parameters, which are suited for use as security measures. Some basic measures are defined in the following:

- Mean Number of Transactions Executed (MNTE) - The mean number of transactions executed in a secure way, before the occurrence of a security compromise;
- Mean Time To Compromise (MTTC) - The mean time elapsed before the occurrence of a security compromise;
- Mean Time Between Compromise (MTBC) - The mean time between the occurrence of security compromises;
- Mean Time To Detection (MTTD) - The mean time elapsed before the detection of a hazard/compromise;
- Mean Time To Removal (MTTR) - The mean time elapsed before the removal of a hazard/compromise.

A fundamental measure is *latency*. Extra care must be devoted to the evaluation of security hazard/compromise latency. In this context, an event is said to be latent if the following conditions hold:

1. It has occurred;

2. It has not been activated (i.e., it has not caused any other remarkable event);
3. It has not been detected (i.e., the system is unaware of it);
4. It has not been removed (i.e., it has not been eliminated from the system).

According to the above definition, it is possible to distinguish between three different kinds of latency, namely:

- Hazard *activation latency* - The amount of time an undetected hazard stays latent, before it is activated (i.e., originates a security compromise);
- Hazard/compromise *detection latency* - The amount of time an hazard/compromise, which is present in the system, stays undetected;
- Hazard/compromise *removal latency* - The amount of time an undetected hazard/compromise persists in the system, before it is eliminated.

The three contributions are shown in Figure 1. In a) an hazard hits a system entity at time t_o (time of *occurrence*) and an operation (which is sensitive to the presence of the hazard in the entity) is performed at time t_a (time of *activation*). The time elapsed between t_o and t_a is the hazard activation latency. In b) an hazard/compromise affects an entity at time t_o and is detected at time t_d (time of *detection*). The time elapsed between t_o and t_d is the hazard/compromise detection latency. In c) an hazard hits the entity at time t_o and is removed at time t_r (time of *removal*). The time elapsed between t_o and t_r is the hazard/compromise removal latency.

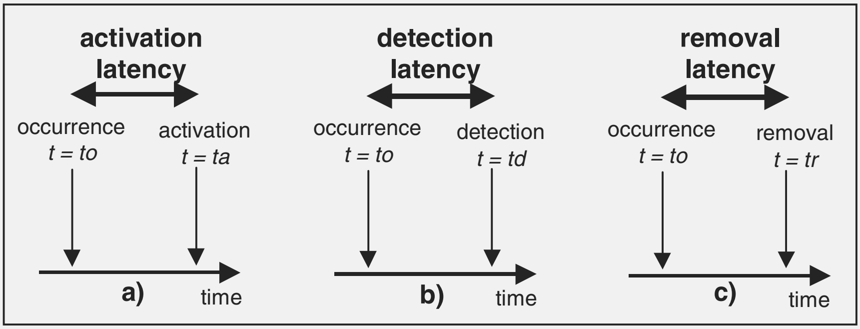


Fig. 1. Contributions to security hazard/compromise latency: a) activation latency - an hazard hits a system entity at time t_o (time of *occurrence*) and an operation is performed at time t_a (time of *activation*); b) detection latency - an hazard/compromise affects an entity at time t_o and is detected at time t_d (time of *detection*); c) removal latency - an hazard hits the entity at time t_o and is removed at time t_r (time of *removal*)

It is worth noting the three contributions may combine in a variety of different ways, thus leading to more complicated scenarios. This makes latency evaluation quite a hard task. Nevertheless, careful investigation of latency data is of foremost importance in many cases, since it makes it is possible to:

- Capture the underlying mechanisms which determine the security level attained by the system;
- Get valuable feedback about the security bottlenecks of the current design;

- Evaluate the effectiveness of possible potential modifications and alternative strategies.

In particular, latency evaluation is of foremost importance in all situations where resolution of disputes depends largely upon the accuracy with which times of events are known. A typical example of such a scenario, in PKI based systems, is the resolution of disputes upon revocation.

5 Hierarchical Simulation

The approach we suggest favors hierarchical simulation. Hierarchical simulation is based on analyzing the system behavior at different levels of abstraction with a simulation sub-model associated to each level. For all levels, the workload might be a real trace file collected on the field, or in alternative it might be generated from a synthetic distribution. The effects of hazards injected at a given level are characterized by statistical distributions and hazard models (e.g., probability and number of hazards affecting a component, and their effects on the component behavior). These distributions are to be used as inputs for hazard injection at the higher level model. As a consequence, hierarchical simulation requires that:

- Distinct levels of abstraction be identified;
- Hazard dictionaries (i.e., a mechanism to propagate hazard effects from lower level models to higher level models) be defined;
- Experimental results from lower levels be propagated to upper levels.

If properly implemented, hierarchical simulation provides extremely detailed modeling of specific aspects at an acceptable computing cost.
However, establishing the proper number of hierarchical levels and their boundaries is not trivial. Several factors must be considered to find an optimal hierarchical decomposition that provides a significant simulation speed up with a minimum loss of accuracy, and in particular:

1. The system complexity;
2. The level of detail of the analysis;
3. The kind of security measures to be evaluated;
4. The strength of system component interactions (weak interactions favor hierarchical decomposition at the opposite of strong coupling).

Simulation for security analysis involves the injection and the propagation of hazards into the system under study at different levels of abstraction, such as the physical level, the system level, the network level, the application level, and the personnel administration level. We envision three fundamental hierarchical levels, which are illustrated in Figure 2. We believe these levels provide an efficient framework for accurate security analysis of a wide class of systems. The simulation, however, can be very time consuming and memory bound, since it has to track the propagation of hazards from lower levels to higher levels.

There are several common issues that apply to hazard injection at all levels. The first issue is: what is the appropriate hazard model at the chosen level of abstraction?

There is no easy answer to this question. Only field data and experience are valuable guides.

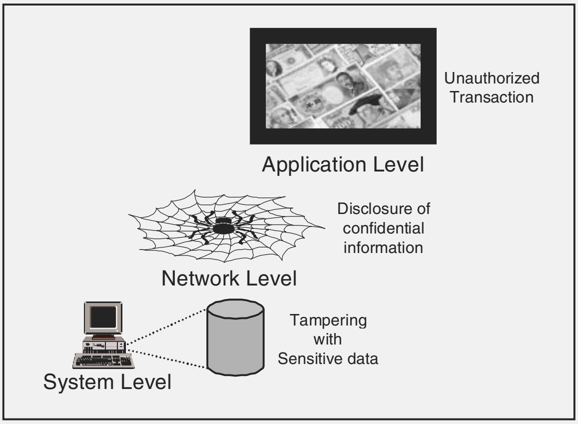


Fig. 2. Hierarchical simulation for security analysis. Hazards propagate from lower levels to higher levels. At the System Level an hazard may be represented by an attacker tampering with sensitive data. This security breach may lead at the Network Level to the disclosure of confidential information. By using such an information, a malicious user might be able at the Application Level to perform an unauthorized transaction

The second issue is: for a given hazard model (e.g. the disclosure of a private key) and hazard type (e.g. transient hazard), where should the hazard be injected? A straightforward approach is to randomly choose a location from the injection space (e.g. all private keys of certificate subjects in the community). This scheme is easy to implement, but it has two major drawbacks. The first is that many hazards may have similar impact (e.g. misuse of private keys of ordinary users may have comparable effects). The second is that many hazard locations may not be exercised at all. An alternative approach is to inject hazards to a few representative locations under selected workload. This technique can be used to evaluate the impact of locations or workloads in terms of system security. Alternative injection strategies should be used, so as to provide a broad evaluation of the system.

6 Tool Architecture

The result of the above discussed considerations is a simulation tool, called SECURE, currently under development at the University of Naples. SECURE is a powerful tool for security analysis, which supports hierarchical and hybrid simulation. It represents a versatile means of evaluating system security as early as in the first design steps. It makes for effective testing, since it is possible to analyze the system under realistic operational conditions, including driving the simulation using real traces collected on the field. The hierarchical approach allows the behavior of components at a given level to be detailed in the lower level model. The granularity of the simulated

activities and the quantitative measures evaluated are refined from one level to another. The tool provides support to rapidly model fundamental components found in most PKI based environments, to represent functional relationships and timing dependencies between them, to inject hazards to system components, to investigate the effects of alternative policies, to mimic the execution of procedures for detection and handling of security compromises, and to evaluate the effectiveness of different protection mechanisms and strategies. This makes it possible to extract quantitative measures, characterizing the probability and the criticality of potential security breaches, and ultimately evaluate the security level attained by the system. System ability to cope with security attacks is evaluated with respect to a number of different factors, and under varying load conditions.

In the following, we describe the structure of the SECURE integrated tool. This structure is illustrated in Figure 3.

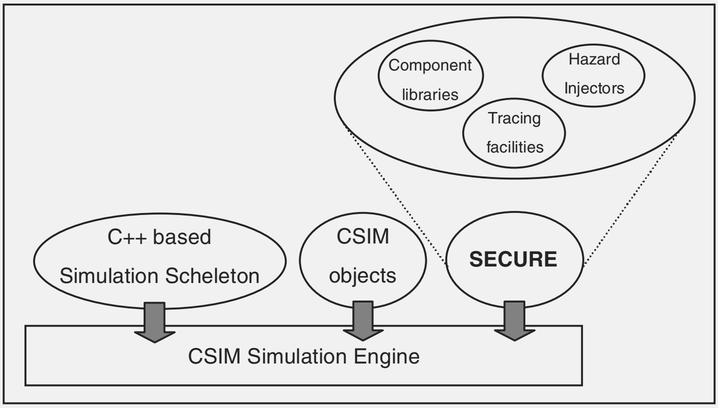


Fig. 3. The SECURE simulation environment. The simulation scheleton defines interactions between simulated system components. C-SIM provides the simulation engine and the basic features to produce estimates of time and performance. SECURE facilities (the Component Libraries, the Hazard Injectors, and the Tracing Facilities) are specifically tailored to addressing security-related issues

As shown in the figure, SECURE incorporates C-SIM [8][9]. C-SIM is a process-oriented discrete-event simulation package for use with C or C++ programs. It provides a convenient tool which programmers can use to create models of a system to produce estimates of time and performance. By incorporating C-SIM objects and features, SECURE is able to take into account performance related issues. The SECURE simulation environment augments CSIM with a number of facilities, specifically tailored to addressing security-related issues. To achieve this, SECURE provides a number of features to evaluate security related aspects.

The main components of SECURE are:

- The component libraries
- The hazard injectors

- The tracing facilities

6.1 Component Libraries

The *component libraries* provide a number of objects and features, which are a generalization of those typically found in most PKI based systems. Since SECURE is intended for use by designers of real PKI systems, the names for the base classes have been chosen as close as possible to the standard ones (we did not want to bother the designers with some new fancy names).
The main object classes of the current implementation are:

- The *Certification Authority* (CA) – Simulates an entity that issues *Public Key Certificates* (PKCs) and Certificate Revocation Lists (CRLs). Certificate applicants may enroll (either directly, or via a Registration Authority) and receive PKCs, which convey identity information about the certificate subject. This is done in accordance to well defined rules, as specified in the policy and in the Certification Practice Statement [10];
- The *Authorization Authority* (AA) – Simulates an entity that issues *Attribute Certificates* (ACs) and Attribute Certificate Revocation Lists (ACRLs). Certificate applicants may enroll (either directly, or via a Registration Authority) and receive ACs, which convey authorization information about the subject of the public key certificate pointed to by the attribute certificate [11];
- The *Registration Authority* - Simulates an entity that front-ends a Certification Authority service or an Authorization Authority service. It is in charge of authenticating certificate applicants, according to the enforced rules;
- The *Relying Party* (or *Certificate User*) - Simulates a party who acts (or is in a position to act) in reliance upon a certificate and its subject public key;
- The *Subscriber* - Represents a party who is the subject of a certificate and who is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate;
- The *Repository* - Is a database of certificates and other relevant information accessible online;
- The *Link* - Comes in two flavors: the *Generic Link* object and the *Secure Link* object. The former acts as a conduit, and is the basic means of communication. The latter is an embellished version of the same object, which provides a secure communication channel between two entities.

6.2 Hazard Injectors

The *hazard injectors* enable the designer to mimic hazard occurrences in the system components according to realistic scenarios. This is achieved by means of a utility class that has the capability of injecting hazards into other objects, thus providing the user with an external mechanism to handle injecting hazards into a large number of components. Such a strategy increases the control one has over the actions of the individual pieces. Since several independent external injectors can be created and

used, this provides the means for simulating quite complex hazard scenarios. In alternative to using an external entity, injectors can be incorporated in the objects. This provides the components with a built-in injection system, which greatly simplifies the simulation. It is up to the user whether to use the simple route, or to employ the more customizable route.

As far as hazard *duration* is concerned, we distinguish between *transient hazards* (i.e., hazards which disappear after some time), and *permanent hazards* (i.e., hazards which persist in the system if proper actions are not taken). A transient hazard occurs, for example, if a private key is disclosed. In this case, the hazard will automatically disappear upon expiration of the validity period of the corresponding public key certificate. The hazard may also be removed prior to the expiration date of the certificate, if this is successfully revoked. A typical example of a permanent hazard is a breach into a system which hosts sensitive data. In this case a security hazard is present until the breach is detected and proper remedy action is taken.

SECURE provides many options to tailor how the injection process acts. For transient hazards, it is possible to set the hazard duration to a constant value, or, for random-duration ones, to set normalcy parameters for the duration and the standard deviation (for normal sampling). It is also possible to have the injector read hazard data from a file collected on the field.

As far as hazard *occurrence* is concerned, different analytical models for both transient and permanent hazards, are available. We can set the injection model to one of a number of predefined types, such as constantly occurring, exponentially based, Weib-distribution based, or Erlang-distribution based. Again, it is also possible to have the injector read hazard data from a file collected on the field.

6.3 Tracing Facilities

To help the designer to evaluate the security level attained by the system or system prototype under test, support has been incorporated into SECURE to extract quantitative measures from experimental data. The *tracing facilities* make it possible to monitor a number of events, and in particular:

- Hazard occurrence – a security hazard manifests in a system component;
- Hazard activation – an hazard, which was present in a system component, leads to a security compromise. An hazard activation thus corresponds to a compromise occurrence;
- Hazard/compromise detection – an hazard/compromise, affecting the system or a system component, is detected;
- Hazard/compromise removal – an hazard/compromise, affecting the system or a system component, is eliminated.

The tracing facilities also provide a number of functions to extract from the collected data the security measures and the latency information described in section 4.

7 Conclusions and Directions of Future Work

This work has presented a novel methodology to system security analysis, called *simulated hazard injection*. The approach consists in simulating the behavior of the target system while hazards, i.e. attacks to system security which may originate security compromises, are injected to its components. To the best of our knowledge, such an approach has never been proposed in the literature before. The methodology is augmented by the definition of a set of parameters, which are suited for use as security measures. Among these, particularly relevant is latency. Extreme detail is needed in the evaluation of the latency of a security hazard/compromise, in order to evaluate the security level attained by the system. The suggested analysis technique and metrics have been integrated in a simulation tool for designing PKI based systems. The tool is called SECURE and it provides support to rapidly model fundamental components found in most PKI based environments, to represent functional relationships and timing dependencies between them, to inject hazards to system components, to investigate the effects of alternative policies, to mimic the execution of procedures for detection and handling of security compromises, to evaluate the effectiveness of different protection mechanisms and strategies, and to extract quantitative measures, characterizing the probability and the criticality of potential security breaches. This ultimately allows the system developer to evaluate the trade-offs of alternative design solutions, with respect to a number of different factors.

Future work will aim at:

- Demonstrating the potentialities of the suggested approach, by applying the methodology and the tool to the case study of a real system;
- Combining the measures provided by the tool, in order to reflect standard criteria for product evaluation (such as, for example, the ITSEC common criteria).

Acknowledgements

This work was supported in part by the *MOSAICO project*, in cooperation with the *Universities of Naples*.

References

1. Ford, W., Baum, M. S.: Secure Electronic Commerce. Prentice Hall Inc., Upper Saddle River (1997)
2. Atkins, D. et al.: Internet Security Professional Reference. 2nd edn. New Riders Publishing, Indianapolis (1997)
3. Iyer, R. K. , Tang, D.: Experimental Analysis of Computer Systems Dependability. In: Pradhan, D. K.: Fault-Tolerant Computer System Design. Prentice Hall Inc., Upper Saddle River (1996)
4. Saleh, R.A., Newton, A.R.: Mixed-Mode Simulation. Kluwer Academic Publishers (1990)

5. Obal II, W. D., Sanders, W. H.: An Environment for Importance Sampling Based on Stochastic Activity Networks. In: Proceedings of the 13th Symposium on Reliable Distributed Systems, Dana Point , CA (1994) 64-73
6. Kaancihe, M., Romano, L., Kalbarczyk, Z., Iyer, R. K., Karcich, R.: A Hierarchical Approach for Dependability Analysis of a Commercial Cached RAID Storage Architecture. In: Proccedings of The Twenty-Eighth Annual International Symposium on Fault-Tolerant Computing (FTCS28), IEEE-CS, Los Alamitos (1998) 6-15
7. Goswami, K. K., Iyer, R. K., Young L.: DEPEND: A Simulation-Based Environment for System Level Dependability Analysis". In: IEEE Transactions on Computers, Vol. 46, No. 1 (1997) 60-74
8. Schwetman, H.: Using CSIM to model complex systems. In: Proceedings of the 1988 Winter Simulation Conference, ed. M. Abrams, P. Haigh, and J. Comfort, San Diego (1988) 246 - 253
9. CSIM18 User Guides (C++ version), http://www.mesquite.com/
10. PKIX Working Group: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. INTERNET-DRAFT, April 1998
11. PKIX Working Group: An Internet Attribute Certificate Profile for Authorization. INTERNET-DRAFT, April 1999

Lazy Infinite-State Analysis of Security Protocols

David Basin

Institut für Informatik,
Universität Freiburg, Germany
basin@informatik.uni-freiburg.de

Abstract. Security protocols are used to exchange information in a distributed system with the aim of providing security guarantees. We present an approach to modeling security protocols using lazy data types in a higher-order functional programming language. Our approach supports the formalization of protocol models in a natural and high-level way, and the automated analysis of safety properties using infinite-state model checking, where the model is explicitly constructed in a demand-driven manner. We illustrate these ideas with an extended example: modeling and checking the Needham-Schroeder public-key authentication protocol.

1 Introduction

The increasing popularity of distributed computing and applications like internet banking and electronic commerce has created both tremendous risks and opportunities. Many of the risks stem from security breaches, which can be ruinously expensive. One of the cornerstones of security is the use of *security* (or *cryptographic*) *protocols* in which information is exchanged that is intended to provide security guarantees such as authentication or atomicity of cash/goods transactions. Although such protocols typically involve each agent sending only a few messages, they are extremely difficult to get right. Designing correct protocols has been likened to "programming Satan's computer" [1] as the protocol should work in the presence of a hostile, powerful, opponent who can read and alter messages at will.

In response to this challenge, various formal methods have been proposed for analyzing security protocols. Many of them are based on either model checking or interactive verification. In model checking[1], systems are modeled as (finite-state) transition systems, where states model protocol events or agent knowledge [7, 12, 16, 17]; the state space can then, at least in theory, be completely analyzed to determine if a desired property holds. Model checking methods are powerful and automatic, but their use as decision procedures often requires strong assumptions to bound the information that is analyzed. This is problematic because there are

[1] We use the term *model checking* in a general way that includes approaches based on explicit state enumeration, e.g. [4], as well as temporal logics and automata theory.

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 30-42, 1999

infinitely many messages that attackers can possibly send. An alternative is to develop specialized logics [2, 11] or approaches for reasoning about protocols that do not bound the possible messages sent. For example, one can model protocols as sets of possible communication traces, where messages of unbounded size can be sent [15]. The disadvantage is that this results in an undecidable formalism and verification requires interactive theorem proving, which demands considerable effort.

In this paper, we present a new approach to protocol analysis that combines complementary aspects of model checking and verification. We show how, in the appropriate setting, the kinds of formal models that are used for interactive verification can also be used for automatic, infinite-state, model checking.

The key idea is that we use *lazy data types* to model the infinite state-space associated with a protocol. A lazy data type is one where data-type constructors (e.g., *cons* for building lists, or *node* for building trees) build data types without evaluating their arguments [6]; this allows us to represent and compute with infinite data (e.g., streams or infinite trees), generating as much of the data as is needed on demand. We use lazy data types to build a model and to compute with it afterwards. We formalize a protocol and attacker model (a description of the powers of attackers) as an infinite tree and perform infinite-state model checking using standard search algorithms combined with heuristics that prune and reorder the infinite tree in a demand driven fashion.

The semantic formalism we use for modeling protocols and attackers is a trace-based interleaving semantics, motivated by, and closely following, the account given by Paulson in [15]. Paulson models a protocol as an inductively defined sets of traces, where each trace is consistent with the protocol and the chosen attacker model. He uses these models for verification: he interactively proves, by induction, that violations of security properties (i.e., some bad situation, such as a spy learning the key of an honest agent) cannot occur in any trace. In our work, rather than formalizing protocols as inductively defined sets, we formalize them as infinite trees. The nodes of the tree are traces and children correspond to trace extensions by a step of (some run of) the protocol or an action by an attacker. Hence, a protocol, along with an attacker model, defines an infinite tree and a security property is a property of nodes in the tree. Violations of security properties are found by a kind of infinite-state model checking, which is performed by searching the infinite tree.

Formalizing inductively defined sets as lazy trees makes it easy to represent the search space in a structured way. During search we explore the infinite tree, constructing finite prefixes of it "on the fly". The result is a formalism, with a clear semantic foundation, that we can directly use for automatic property checking. Moreover, the use of lazy trees makes it easy to incorporate heuristics into model checking: we use heuristics to lazily reorder the infinite tree, producing dramatic speedups in subsequent search.

The remainder of this paper is organized as follows. In section 2 we provide an overview of the semantic formalism used in this paper and some background on lazy data types and Haskell, a lazy language that we use for our work. We

$$\begin{array}{ll} s_1) & A \to B : \ \{A, N_A\}_{K(B)} \\ s_2) & B \to A : \ \{N_A, N_B\}_{K(A)} \\ s_3) & A \to B : \ \{N_B\}_{K(B)} \end{array}$$

Fig. 1. Needham-Schroeder public-key authentication protocol

also introduce our running example: the Needham-Schroeder public-key authentication protocol. In section 3 we explain how we formalize models of protocols and in section 4 we show how to carry out model checking with them. We also discuss heuristics and present experimental results. Finally, in section 5, we draw conclusions.

2 Background

2.1 From protocols to traces

A protocol is a recipe that describes how *agents* (or *principles*) should act to achieve some goal. Protocols are often described using informal notation, for example as a sequence of instructions explaining the actions taken by the agents. Figure 1 is a typical textbook account of a protocol, in this case, a version of an authentication protocol proposed by Needham and Schroeder [14]. The protocol consists of three steps (s_1–s_3) in which two agents, A and B, exchange messages in order to mutually authenticate each other.

Each step describes an *event* $A \to B : X$, which states that A exchanges the message X with B. Messages consist of atoms, like agent names and nonces (randomly generated strings), and are composed by tupling. Moreover, messages may be encrypted using keys of agents. Here, in the first step, A identifies himself and sends a nonce N_A to B. The entire message is encrypted with B's public key. In the second step, B sends N_A back to A, along with his own nonce N_B, encrypted with A's public key. Sending N_A back authenticates B: for only B could return N_A, at least if we assume (1) perfect encryption, (2) that only B knows his private key, and (3) that other agents cannot simply guess the nonce N_A. B also sends along his own challenge, the nonce N_B, which A returns in the third step, thus demonstrating that she is really A.

Although security protocols are small and appear intuitive, this appearance is deceptive. The above protocol was proposed in 1978 and twenty years went by before [10] discovered that, contrary to what was believed, the final step of the protocol does not authenticate A; it is possible for B to finish a run of the protocol with an agent who is other than she claimed to be in the first step. These kinds of errors, which can be exceedingly subtle, motivate the need for formal analysis. By giving a protocol a formal semantics we can then make meaningful statements about whether it has desired properties. Moreover, a formal semantics is the basis for rigorous analysis based on verification or, in our case, model checking.

$$\frac{}{\langle\rangle \in P}\ \mathit{empty} \qquad \frac{t \in P \qquad N_A \notin \mathit{used}\ t}{t,\ \mathbf{A} \to \mathbf{B} : \{\mathbf{A}, \mathbf{N_A}\}_{\mathbf{K_B}} \in P}\ s_1$$

$$\frac{t \in P \qquad N_B \notin \mathit{used}\ t \qquad \mathbf{A}' \to \mathbf{B} : \{\mathbf{A}, \mathbf{N_A}\}_{\mathbf{K_B}} \in t}{t,\ \mathbf{B} \to \mathbf{A} : \{\mathbf{N_A}, \mathbf{N_B}\}_{\mathbf{K_A}} \in P}\ s_2$$

$$\frac{t \in P \qquad \mathbf{A} \to \mathbf{B} : \{\mathbf{A}, \mathbf{N_A}\}_{\mathbf{K_B}} \in t \qquad \mathbf{B}' \to \mathbf{A} : \{\mathbf{N_A}, \mathbf{N_B}\}_{\mathbf{K_A}} \in t}{t,\ \mathbf{A} \to \mathbf{B} : \{\mathbf{N_B}\}_{\mathbf{K_B}} \in P}\ s_3$$

$$\frac{t \in P \qquad X \in \mathit{synthesize}\ (\mathit{analyze}\ (\mathit{sees}\ t))}{t,\ \mathit{Spy} \to B : X \in P}\ \mathit{attacker}$$

Fig. 2. Protocol as inductively defined set

One way to model a security protocol, which is also popular in modeling other kinds of protocols, is to abstract away any possible implementation of the steps and instead to focus on communication between agents: one describes, like in figure 1, the externally observable events that take place and the order in which they occur. No further assumptions are made such as when an event occurs, or how the events of different runs of the protocol between different agents in a network are temporally ordered. Hence, a natural model of a protocol is the set of all possible *traces*, that is, the event sequences that can result from any interleaving of (possibly partial) runs.

It is a relatively straightforward to build a formal model based on this idea. This has been done by Paulson, who completely formalizes such a model in higher-order logic, which he uses for machine supported verification. In his work, a protocol plus an attacker model corresponds to an inductively defined set of traces. Such an inductively defined set can be presented by a collection of rules and is the smallest set closed under application of the rules.

Figure 2 contains the rules Paulson uses to formalize the Needham-Schroeder protocol. Explaining this in detail would take us too far off topic, but the idea is simple enough. The rules define a set of traces P, which constitute the semantics of the protocol. The rules should be read that when the premises (above the line) hold, then the conclusion (below the line) also holds. They formalize how, when certain conditions hold, traces can be extended with new events.

The rule *empty* starts off the inductive definition: the empty trace always belongs to P. This models a system where no communication has (yet) taken place. The rules s_1–s_3 formalize the identically named steps of the protocol. For example, s_1 formalizes that any trace $t \in P$ can be extended (“,” is used to extend the trace t by an event) by the event $A \to B : \{A, N_A\}_{K_B}$. That is, independent of what events have come before, any agent may start a run of the protocol with any other (here terms like A and B are variables that range over all agents). The premise $N_A \notin \mathit{used}\ t$ formalizes that the nonce N_A is fresh, i.e., it doesn't appear in any previous event in the trace t. We have used **boldface**

font to highlight the similarity with the steps in figure 1. The rules s_2 and s_3 explain how, provided the previous steps have occurred (i.e., are contained in the trace), the next step can occur. Note that in s_2 (and similarly in s_3), for B to say $\{N_A, N_B\}_{K_A}$ to A, we require that B received $\{A, N_A\}_{K_B}$, but not necessarily from A. It could be any agent, masquerading as A. Said another way, B cannot, from this message alone, determine who sent it — this is the whole point of authentication! The rule *attacker* formalizes a commonly used attacker model due to Dolev and Yao [5]: the spy can say (and hence augment any trace t) anything that he can synthesize from analyzable parts of messages that he can see. The auxiliary functions *synthesize*, *analyze* and *see* are defined over traces and sets of messages, and we will shortly give our own definitions of them.

To summarize, the rules formalize how traces can be extended with new events in a way consistent with the protocol and together they define the set of all possible communications where protocol runs can be interleaved with each other as well as attacker broadcasts. Hence a protocol corresponds to a set of traces and this provides a basis for formal analysis. A protocol then has [or lacks] some property, precisely when the property holds [or fails] for every [some] trace in the corresponding trace set.

2.2 Lazy Data Types and Haskell

In verification, we can formalize and reason about infinite sets. However, the kinds of constructs available for doing so (e.g., inductive definitions or set comprehension) are usually not available in programming languages where expressions should be computable. However, programming languages offer other possibilities for representing infinite objects: we can write functions that enumerate the elements of infinite sets, at least until we run out of memory or patience. In this sense, a function can represent an infinite set or infinitely large data.

Lazy data types provide a principled way of representing infinite data using functions that can generate arbitrarily large finite prefixes on demand. The term *lazy* derives from the mechanism of lazy evaluation, which ensures that expressions or components of structures are expanded in a demand driven way and are not evaluated more than is necessary to provide a value at the "top level". In a lazy functional programming language this allows us to write recursive definitions that represent infinite data. For example, if ":" is the "cons" constructor for building lists, the two equations

```
nat = from 0
from n = n : from (n+1)
```

define `nat` to be the infinite list `[0,1,2,3,4, ...]`. The cons constructor can be viewed as a function that does not evaluate its arguments until they are required. Hence the elements of this list are generated on demand; only when we ask for the head of the list is the definition of `from` unfolded to generate the first element 0. Evaluation of the remainder (the tail) is again delayed, until computation forces further evaluation.

Lazy data types are extremely useful. We use them to specify the infinite trace sets associated with protocols. We execute these specifications and functions over them using Haskell [8], which is a lazy, higher-order, polymorphically typed, functional programming language. The equations for `nat` given above, and indeed all text in this paper in `typewriter font`, are Haskell programs.

An introduction to Haskell is outside the scope of this paper. However most aspects of Haskell should be clear from the examples given, at least if the reader is familiar with modern functional programming languages. We briefly mention one feature though, which turned out to be very useful for describing protocols. Haskell supports a notation for specifying (possibly infinite) sets using *list comprehension*, which is analogous to *set comprehension*. Sets in Haskell are represented by lists. For example we can represent the set

$$\{2 \times x \mid 1 \leq x \leq 10 \land x \; mod \, 2 = 0\}$$

in Haskell as

```
[2 * x | x <- [1 .. 10], x `mod` 2 == 0]
```

which is equal to $\{4, 8, 12, 16, 20\}$. The notation `[c | t <- xs, p]` represents a set where for each `t` in the list `xs`, for which the predicate `p` holds, we add an element `c` to the result set. In general, there can be more than one *generator* (expressions like `t <- xs`) as well as zero or more predicates. Moreover, in a generator, the term `t` can be a composite term, called a *pattern*, which is matched against each element of `xs`. Due to technical reasons, patterns in Haskell must be *linear*, which means that each variable in `t` can occur just once. One can often work around this by renaming common variables apart and adding predicates that equate them, e.g., translating the generator `[x,x] <- xs` (which selects all doubleton lists from `xs` whose elements are identical) to `[x,x1] <- xs, x == x1`. We will see applications of this shortly.

3 Model building

In the previous section we have described two ideas: how a protocol can be modeled as an infinite set of traces and how to represent and compute with infinite data. We now put these ideas together and show how to formalize protocol models using lazy data types. For concreteness, we return to our running example, the Needham-Schroeder protocol; the ideas are more general.

As observed in the introduction, our formalism is based on Paulson's, except we formalize inductive definitions in a way that we can directly compute with. Moreover, rather than formalizing an infinite set, we formalize an infinite (trace) tree. The difference is slight: each node in the tree is labeled with a trace in the inductively defined set of traces and the layers of the tree correspond to stages of the inductive definition. The advantage over a formalization based on implementing infinite sets as lazy lists is that it is easier to compute the closure of a set represented as a tree since, for a monotone closure operator, the elements

```
s1 t = [(Says a b (Crypt b (Pair (Agent a) (mkNonce t) )))
         | a <- [Alice,Bob,Spy],  b <- [Alice,Bob,Spy], a /= b]

s2 t = [Says b a (Crypt a (Pair (Nonce na) (mkNonce t))) |
         Says _ b (Crypt b1 (Pair (Agent a) (Nonce na) )) <- t,
         b == b1]

s3 t = [Says a b (Crypt b (Nonce nb)) |
         Says a b (Crypt b1 (Pair (Agent a1) (Nonce na) )) <- t,
         a == a1, b == b1,
         Says _ a' (Crypt a1' (Pair (Nonce na') (Nonce nb))) <-t,
         a == a', a' == a1', na == na']

attacker t = [Says Spy a msg | a <- [Alice,Bob],
          msg <- synth(analz Spy (sees Spy t))]
```

Fig. 3. Functions for generating the trace set

introduced at each iteration correspond to the next ply of the tree. This makes it easy to generate the set, without checking for repetition, and, as we will later see, to introduce search heuristics.

The central data type in our work is that of a tree labeled with elements of some type `a` (`a` is a type variable, so we can have trees labeled by elements of arbitrary types). To allow for arbitrarily many children, each node contains an element of type `a` and a list of zero or more trees of type `a`.

```
data Tree a = Node a [Tree a]
```

For example `Node 1 [Node 2 [], Node 17+18 []]` belongs to the type `Tree Int`. Note that `Node` is a lazy data constructor: its arguments (e.g., `17+18`) are evaluated later, only when required for computation.

We use data types to model agents, messages, and events. For the Needham-Schroeder protocol, we formalize three agents, `Alice`, `Bob`, and a `Spy`. Messages may be agent names, nonces, pairs of messages, or encrypted messages. Events are broadcasts of a message from one agent to another.

```
data Agent = Alice | Bob | Spy
data Msg = Agent Agent | Nonce Int | Pair Msg Msg | Crypt Agent Msg
data Event = Says Agent Agent Msg
```

Note that we abstract away from the details of cryptography and identify the public key of an agent with his name (and we will assume that only that agent has the inverse private key). Also, nonces are named by integers.

Figure 3 contains our formalization of the steps of the protocol and the attacker model, based on the inductive definition of figure 2. The functions correspond to the identically named rules: each function specifies how a trace `t` can be extended. For example, `s1` uses set comprehension to iterate over all pairs of agents `a` and `b` (`a` and `b` are variables ranging over agents) and states that

```
analz a hs =
  let inj  xs = xs
      fst  xs = [x | Pair x y <- xs]
      snd  xs = [y | Pair x y <- xs]
      decrypt xs = [x | Crypt ag x <- xs, ag == a]
  in closure (inj `or` fst `or` snd `or` decrypt) hs

synth hs =
  let inj  xs = xs
      agent _ = [Agent a | a <- [Alice,Bob,Spy]]
      crypt xs = [Crypt a x | x <- xs, a <- [Alice,Bob]]
      pair xs = [Pair x y | x <- xs, y <- xs]
  in (inj `or` agent `or` crypt `or` pair) hs

sees a t = foldr (\x r -> (sees1 x) `union` r) emptyset tr
  where sees1 (Says _ b x) = if a == b || a == Spy then [x] else []

or f g = \xs -> (f xs) `union` (g xs)
```

Fig. 4. Formalizing the attacker's capabilities

the event `Says a b (Crypt b (Pair (Agent a) (mkNonce t)))` can be used to extend any trace. The auxiliary function `mkNonce` generates a fresh nonce (not occurring in the trace `t`); hence this formalizes $A \to B : \{A, N_A\}_{K_B}$. The function `s2` (and similarly `s3`) formalizes that an extension corresponding to the second step of the protocol is allowed only when the trace contains the first step.

The last function, `attacker` formalizes the attacker model. This uses the auxiliary functions given in Figure 4.[2] The function `analz` decomposes messages into their analyzable parts, e.g., the parts of pairs. Looking into an encrypted messages requires the corresponding key (so we assume perfect cryptography). We use `synth` to build messages from known parts and `sees` formalizes that the spy can see all communication that has taken place (i.e., is in the trace).

To formalize the model itself, we employ a function, which given (1) an initial state, `init`, and (2) a function, `extension`, mapping states to lists of successor states, formalizes an infinite tree.

```
build_tree extension init
```

[2] In addition, `closure` takes a function `f` and a set `s` and applies `f` to `s` until a fixedpoint is reached. Not that our formalization differs here slightly with respect to Paulson's. He computes the closure in both `synth` and `analz`, whereas we only compute the closure in `analz`; the former is always infinite and the latter is always finite. Formalizing an infinite set is not a problem in a lazy setting; we could do this with a stream. However, we have avoided this as it would result in an infinitely branching tree (instead of a finite branching tree with infinite length branches), which would complicate the application of reordering heuristics. Instead, we perform just one synthesis step, and spread the closure computation down (instead of across) the infinite tree.

```
   = Node init (map (build_tree extension) (extension init))
```

The root of the tree is labeled by `init` and, at each ply, `extension` is applied to generate the successors, upon which `build_tree` is recursively applied. Depending on the extension function, `build_tree` formalizes a tree of finite or infinite depth, which is finitely or infinitely branching.

We complete our specification by applying the above function to formalize `p`, the model itself. The initial state consists of the empty trace and the extension function computes successor states by extending traces using the functions in figure 3.

```
ext t =  map (\x -> ins x t) extensions
          where extensions = ((s1 `or` s2 `or` s3 `or` attacker) t)

p =  build_tree ext []
```

The specification of the model is direct and concise. The corresponding Haskell code takes just over a page.

4 Model-checking

We have formalized an infinite-state model as a lazy tree. Here we show how to perform infinite-state model checking based on lazy state-enumeration: we can search the state space for attacks, constructing parts of the tree on demand. For protocols/attacker models that produce infinite trees, this constitutes a semi-decision procedure. It is a decision procedure when the trees are finite.

If there is an attack, it will be present in a trace located at some node in the tree `p`. Finding this node, however, may not be easy. The tree is not only infinitely deep, it has a large branching factor. For example, the first ply has 12 nodes; each node contains a singleton trace and together the 12 traces represent all the ways that any two distinct agents can start a run of the protocol as well as all the messages that the spy can send.

```
[Says Alice Bob (Crypt Bob (Pair (Agent Alice) (Nonce 0)))]
[Says Alice Spy (Crypt Spy (Pair (Agent Alice) (Nonce 0)))]
[Says Bob Alice (Crypt Alice (Pair (Agent Bob) (Nonce 0)))]
[Says Bob Spy (Crypt Spy (Pair (Agent Bob) (Nonce 0)))]
[Says Spy Alice (Crypt Alice (Pair (Agent Spy) (Nonce 0)))]
[Says Spy Bob (Crypt Bob (Pair (Agent Spy) (Nonce 0)))]
[Says Spy Alice (Agent Alice)]
[Says Spy Alice (Agent Bob)]
[Says Spy Alice (Agent Spy)]
[Says Spy Bob (Agent Alice)]
[Says Spy Bob (Agent Bob)]
[Says Spy Bob (Agent Spy)]
```

(Note that for the empty trace, the spy is unable to say much of interest — this quickly changes as the traces grow.) The second ply has 314 nodes and the

```
sortPly f t = mapBranches f t
   where mapBranches f (Node a l) = Node a (map (mapBranches f) (f l))

p' =  sortPly f (prune p)
  where f = sortBy cmp
        cmp (Node t1 _) (Node t2 _) =
               if w1 < w2 then LT
               else if w1 == w2 then EQ else GT
                      where w1 = weight (head t1); w2 = weight (head t2)
        weight e = (protStep e) + (fromSpy e)
        protStep (Says _ x (Crypt x1 (Pair (Agent _) (Nonce n) ))) =
               if x == x1 then 1 else 10
        protStep (Says _ a (Crypt a1 (Pair (Nonce na) (Nonce nb)))) =
               if a == a1 then 2 else 10
        protStep (Says _ b (Crypt b1 (Nonce nb))) =
               if b == b1 then 3 else 10
        protStep _ = 10
        fromSpy (Says a1 a2 _) =
               if (a1 == Spy || a2 == Spy) then 0 else 4
        prune t = filterBranches (\x -> protStep (head x) <= 3) t
```

Fig. 5. Heuristics for pruning and reordering the tree

third 17,529. Such an exponential branching factor means that standard search algorithms are unlikely to succeed in finding even relatively simple attacks that might reside at shallow depths. Therefore, we use heuristics both to prune the search tree as well as to reorder the way it is searched.

Figure 5 displays the heuristics we use, which are based on two simple ideas. First, the protocol specifies events of a particular format: agents taking part in the protocol only send certain kinds of messages. The spy, however, has considerably more freedom and, as a result, many traces contain events that could not have resulted from some step of the protocol and have no consequences as they will not provoke any response from honest protocol participants. The first heuristic is to prune these traces and their successors. Second, we assign priorities to events and give the highest priority to those that could arise from the first step of the protocol followed by the second and then the third. Moreover, we give events a higher priority when they involve the spy. This priority is input to a function, `sortPly`, which sorts, according to priority, the nodes on a ply.

Applying the heuristics to `p` yields `p'`. The use of lazy data types here allows us to separate search from pruning and ordering heuristics: conceptually, the heuristics map the infinite tree `p` into another, `p'`, which we can later search. In reality, lazy evaluation applies the heuristics in a demand driven way during search to explore first parts of the tree that contain potentially interesting dialogs with the spy.

We model check the improved search space using standard search algorithms. We found most useful an implementation of iterative deepening search, `ids`, that iterates bounded depth first search with bounds 0, 1, 2, ...

```
ids pred t = flatten [ idsn n pred t | n <- [0 ..]]

idsn n pred (Node a l) =
 if   n == 0 then (if pred a then [a] else [])
 else if pred a then (a:rest) else rest
      where rest = flatten (map (idsn (n-1) pred) l)
```

The result returned by `ids` is a stream (lazy list) of states for which `pred` holds.

Formalizing an appropriate instance of `pred` that characterizes security violations turned out to be surprisingly difficult. Attacks manifest themselves as traces where the spy learns secrets, or takes on identities, which he shouldn't and it is non-trivial to characterize such traces in a general, high-level, way. In our case, we encoded specialized predicates over traces to formalize violations of particular security properties. For example, we can formalize "after a run of the protocol, B fails to authenticate A" as: agent B gets a nonce from (an agent claiming to be) A in format of step 3 (so the run is complete) that he sent to a different agent C in format of step 2, which the spy can analyze.

```
attack [] = False
attack (Says a b (Crypt b1 (Nonce nb)):tr) =
 if b == b1 then (sent tr && analyze) else attack tr
 where sent [] = False
       sent (Says b2 c (Crypt c1 (Pair (Nonce _) (Nonce nb1))):esrest) =
            (b1 == b2 && nb == nb1 && c == c1 && c /= a && c /= b)
                || sent esrest
       sent (_:esrest) = sent esrest
       analyze = elem (Nonce nb) (analz a (sees Spy tr))
attack (_:tr) = attack tr
```

With all the pieces in hand, we can now model-check. The command

```
head(ids attack p')
```

applies `ids` to the optimized tree, and `head` forces the computation of the first element of the stream, which is returned as the result. The result of this search is a trace that represents a version of the "man in the middle" attack on the Needham-Schroeder protocol, first identified by [10].

```
[Says Alice Spy (Crypt Spy (Pair (Agent Alice) (Nonce 0))),
Says Spy Bob (Crypt Bob (Pair (Agent Alice) (Nonce 0))),
Says Bob Alice (Crypt Alice (Pair (Nonce 0) (Nonce 2))),
Says Alice Spy (Crypt Spy (Nonce 2)),
Says Spy Bob (Crypt Bob (Nonce 2))]
```

The trace, read top down, lists the events that constitute the attack. In this attack, Alice starts the protocol (first step) with the Spy. The Spy takes advantage

of this by starting another run of the protocol with some other agent, here Bob, passing on Alice's message. When Bob responds with his own nonce (third step), Alice assumes that it came from the spy.[3] She then sends back the nonce to the Spy (fourth step) who uses it to convince Bob that he is Alice (fifth step). This attack shows that if Alice talks to someone who has the powers of an attacker, then this can be used to take on her identity. Hence, this protocol is too weak to actually authenticate the initiator.

This attack, which involves a trace of length 5, is found on the fifth ply of `p'`; the search requires 13 CPU seconds on a 400 Megaherz PC. Model checking with pruning, but no reordering, finds a solution in just over a minute. Without pruning, our computing resources were inadequate to find an attack.

5 Conclusions

Semantic models provide a foundation for interactive verification. We have shown how such models, in the context of a lazy programming language, can be used to formalize and automate the analysis of security protocols. Our empirical results are encouraging and provide evidence for the suitability of our approach.

There are a number of directions for future work. First, we would like to carry out more ambitious case studies. To support this, it would help to be able to generate formal models from high-level descriptions (as in figure 1) of security protocols and attacker models; furthermore, it should be possible to use these descriptions to generate automatically search heuristics like those we considered. Second, our formalization of the `attack` predicate in section 4 is ad hoc. We would like to develop more principled, high-level, ways of specifying security properties. Perhaps using predicates about agent belief, like those in the BAN logic [2], could help, although work is required to give such predicates meaning with respect to the kinds of models we used. Finally, we have shown that it is possible to take models from verification and recast them in a setting where they become more computable. The result, of course, is still completely formal. Hence, it would be interesting to use our models for both model checking and inductive theorem proving.

References

1. R. Anderson and R. Needham. Programming Satan's computer. In *Commputer Science Today*, volume 1000 of *LNCS*, pages 426–441. Springer-Verlag, 1995.

[3] For those familiar with Lowe's attack, our third step corresponds to two steps in his attack: (1) Bob sends his message to the Spy and (2) the Spy sends the message on to Alice. One can check that under our modeling, these two steps can indeed be merged: Alice cannot tell who sends her the message in step three, so it does not matter whether it comes from Bob or the Spy. All that matters to Alice is that it is in the format of step two for her run with the Spy; since it is, she answers with step three.

2. Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Transactions in Computer Systems*, 8(1):18–36, 1990.
3. John Clark and Jeremy Jacob. A survey of authentication protocol literature: Version 1.0. Available at the URL `http://www.cs.york.ac.uk/~jac/`.
4. G. Denker, J. Meseguer, and C. Talcott. Protocol specification and analysis in Maude. In N. Heintze and J. Wing, editors, *Proceedings of the Workshop on Formal Methods and Security Protocols*, pages 939–944, Indianapolis, Indiana, June 1998.
5. D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29:198–208, 1983.
6. Dan P. Friedman and David S. Wise. Cons should not evaluate its arguments. In S. Michaelson and R. Milner, editors, *Automata, Languages and Programming*, pages 257–284. Edinburgh University Press, 1976.
7. Nevin Heintze, J.D. Tygar, Jeannette M. Wing, and Hao-Chi Wong. Model checking electronic commerce protocols. In *Proceedings of the USENIX 1996 Workshop on Electronic Commerce.* 1996.
8. P. Hudak, S. Peyton Jones, and P. Wadler (Editors). Report on the programming language Haskell: A non-strict, purely functional language (version 1.2). *ACM SIGPLAN Notices*, 27(5), 1992.
9. Richard Kemmerer, Catherine Meadows, and Jonathan Millen. Three systems for cryptographic protocol analysis. *Journal of Cryptology*, 7(2):79–130, 1994.
10. Gawin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Proceedings of TACAS'96*, LNCS 1055, pages 147–166. Springer, Berlin, 1996.
11. Wenbo Mao. An augmentation of BAN-like logics. In *Proceedings of the 8th IEEE Computer Security Foundations Workshop*, pages 44–56. IEEE Computer Society Press, 1995.
12. W. Marrero, E. Clarke, and S. Jha. Model checking for security protocols. In *Proceedings of the DIMACS Workshop on Design and Verification of Security Protocols.* 1997.
13. Jonathan K. Millen, S.C. Clark, and S.B. Freedman. The Interrogator: Protocol security analysis. *IEEE Transactions on Software Engineering*, 13(2):274–288, 1987.
14. Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.
15. Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.
16. A.W. Roscoe. Modelling and verifying key-exchange protocols using CSP and FDR. In *Proceedings of 1995 IEEE Computer Security Foundations Workshop.* IEEE Computer Society Press, 1995.
17. Steve Schneider. Verifying authentication protocols in CSP. *IEEE Transactions on Software Engineering*, 24(9):741–758, 1998.

lec r ic e s: ere e fr ere?

arkus akobsson , a id aihi , Yiannis siounis , and oti Yung

f a Sc e ce Re ea ch e e , e ab , a , e e e 4
www.bell-labs.com/user/markusj
e , ag D e, S e , Re , 4 5
david.mraihi@gemplus.com
S e a h c , c , e Y , Y yiannis@spendcash.com
e , c , e Y , Y moti@certco.com

t t. e , he e e a he e eb - e b e b g, h affic, a e g a c e g g a a e e e a a e e e , he f e a f - e c - e ce ha bee b e ea e e he ac f c e e a ec e e ec c a e e h e g , f b g e-g a a g h e- e h gh beca e c ea e ea ha a f a e be afe a effic e , a a e g c ca e e e e , he ca e ha he e e a e e h f ch ce a ha f a a c e ca De e he e ea e a a e e e a , he e ha e a be f g fica - a a h c g , c g ac f ec , ac f a , ab each a a e ce e c e e e e , a ge e hea h e ec a e , a he e a e effic e c ce g a a e a
The e a e f h ch a e e e he ea e he e g f a e a e e ec c a e e e ea he e e age – e e bef e he c ce f he e eb S ch e g e he ec , a , effic e c , a e a a ea f ca h a ac , b a e ec c f S e ea che e , ch a he e e b a , e e b a he c e ca c e he , ch a he che e e e e b D g a h, ffe e a h c g a h c ec a a e a S he , ch a ce , ce c a e e e , e f he e e a age fe a e he a e ace, a ha e e he cea e e ha e eache a e a e ce
Th a e a c a e h a a e c h e e a - e he ea h he e a a e-c e ce a e ha e ec e e , a gge e a f e ec c a e be e e he e e , a g he b e he e c e ca a ac The e f h a e e he age f ch a - c b e e g, b ef, e f he a e che e c e a a ab e a c e f he ba c b e he a ea

a , e-ca h, e-c e ce, e ec c a e , ec -

. au gar (d.): ’ 7 pp. – .

r c i

uit a larg numb r of ars had pass d from th introduction of rpan t/Int r- n t until it start d to b com cl ar that th Int rn t ould b com a hicl for carr ing -comm rc . In th b ginning, this n t ork as larg l of militar int r st and us d b acad mics, and traffic as limit d to mail and fil trans- f rs using `ftp`. arg collaborati distribut d computing as thought to b an application, but did not mat riali . With th introduction of as to us us r int rfac s bas d on `HTML`, acc ss b cam possibl for th mass s, causing both th numb r of us rs and th int r st in conducting comm rc to gro rapidl . On of th n t major st ps hich promis s to bring a larg incr as in Int rn t us and ff cti n ss is an impro d pa m nt infrastructur (in a r g n ral s ns). On factor commonl b li d to ha damp n d th possibiliti s for, and int r st in, l ctronic comm rc has b n th lack of such an infrastructur . hus, practicall mplo abl -comm rc has to dat b n bas d on isting pa m nt structur s, i . cr dit cards. h s ho r, ha s ral prop rti s that mak th m inappropriat for us o r th Int rn t; som of th s includ th ir larg o rh ad, risks r lat d to inappropriat us , and incon ni nc of us - particularl for small pa m nts.

o, it s ms that alt rnati and simpl r m thods of pa m nt ar r quir d. h lack of such simpl sch m s can b plain d b “th chick n and th gg probl m,” nam l , ithout a larg isting m rchant bas , th n d for pa m nt sch m s is l ss acut , and ithout a orking pa m nt sch m , m rchants ar unabl to nt r th Int rn t mark t. noth r probl m has b n that financial institut s traditionall ar r cons r ati , particularl h n it com s to tr ing out n and h r tofor unpro n pa m nt m thods.

ll of th s probl ms ar , ho r, graduall fading a a : substantial ork is b ing p rform d on impl m nting public k infrastructur s. rchants ar b coming a ar of th strong pot ntial of th Int rn t mark tplac and ar making th ms l s r ad to nt r it quickl , and som banks ar starting to m- plo cr ptograph rs and s curit p rts, making it asi r for th m to aluat t chnolog -r lat d risks.

It s ms that it is no long r a qu stion h th r th r ill b W b-bas d pa m nt sch m s. Ho r, a qu stion that r mains is hat t p of sch m (s) ill b mplo d and ho soon. o som t nt th qu stion of hat sch m s ill b dominant ma b r sol d not b th consum r, but ia go rnm nt int r ntion and bank pr f r nc s, and b corporat sponsorship. It is lik l , though, that man sch m s ill co- ist at l ast for a f ars, allo ing th consum r to stat d sir d pr f r nc s.

r ptographic r s arch has produc d s ral important pa m nt r lat d no- tions and prop rti s of sch m s o r th last f ars. h s includ , among oth rs, th issu s of anon mit , r okabl anon mit and fairn ss, crim pr n- tion, micropa m nts, smart card and bas d sch m s, soft ar -onl sch - m s. It s ms that much has b n achi d, t sinc global or id usag has not b n achi d, it ma b th cas that th r is still a lot of n issu s to b d alt ith and much t chnological ork to b don . his is an int r sting

issu that n ds to b discuss d and amin d. h suitabilit of th r s arch r sults to th actual probl ms fac d b financial institutions and th m rchant bas is anoth r moti ating issu . his gi s ris to th follo ing charact ri ation of cat gori s.

. a t at g ri s

t this point should clarif that l ctronic pa m nts can b classifi d according to th acting parti s. h parti s can b busin ss-to-busin ss, consum r-to-busin ss, busin ss-to-consum r, busin ss-to-go rnm nt, tc. Ho r, most of th s l ctronic pa m nt n ds ha b n co r d. usin ss s can transf r funds to ach oth r ia H or Wir transf rs. imilarl , th can transf r funds to go rnm nts. urth rmor , n though th r is still th possibilit of nabling l ctronic ch cks among th s ntiti s, it is still uncl ar h th r or not this is an nhanc m nt of curr nt possibiliti s or simpl a tru busin ss nabl r. uch of th busin ss r lat d pa m nts and comm rc ma r l on s st ms hich follo bank-aid d busin ss to busin ss practic s hich ma b construct d as nhanc m nts to "public-k infrastructur ," as oppos d to on d dicat d pa m nt s st ms. th "four-corn r mod l" of t pical comm rc banking transactions that as put forth in [K Y9].

It s ms to us that th op n probl m d manding imm diat att ntion in curr nt l ctronic pa m nt m thods is th lack of ffici nt consum r ori nt d pa m nt m thods (ith r consum r to busin ss or busin ss to consum r). his pap r and discussion is th r for focus d on this particular part of th mark t (of cours , this s gm nt of pa m nts has to b conn ct d to oth r -pa m nts).

rga i ati

h pap r is organi d as follo s. ction 2 discuss s cr dit cards, hich ar b far th most promin nt m thod for l ctronic pa m nts. ction 3 discuss s l ctronic ch cks, and ho th fit in th on-lin pa m nt ar na. ction 4 cat gori s th arious propos d "cash-lik " m thods. ction 5 gi s r pr s ntati ampl s of a ari t of pa m nt s st ms. W ob iousl ar not hausti in co ring th man arious sugg st d sch m s and apologi for omitting man int r sting d signs. om of th busin ss and political issu s ar m ntion d in ction 6. h n, ction 7 touch s on som possibl futur sc narios, constraints and implications. ction conclud s th pap r.

re i r e s

h most common t p of pa m nt us d on-lin ar cr dit card pa m nts. h main r asons for this is of cours con ni nc , as of us , and b caus th th ar ubiquitous and omnipr s nt. Ho r, as not d abo , th ar ins cur , off r no anon mit , and do not allo small pa m nts.

- **ig c sts a i abi it t a s a pa ts.** ach cr dit card pa m nt has a fi d cost of 2 -4 c nts, plus a ariabl cost of 2-4.5%, d p nding on th m thod us d and th n gotiat d contract.
  h fi d costs originat from th cost of p rforming a transaction, sinc transactions usuall in ol som t p of pap r ork, and th tra rsal of a propri tar n t ork r nt d b isa, ast rcard, or som oth r cr dit card pro id r. U banking r gulations ist hich mandat that us rs' accounts b maintain d so as to nabl a m chanism for disputing pa m nts. his mak s r lati l high fi d costs una oidabl .
  h ariabl costs ar a r fl ction of th s curit probl ms associat d ith cr dit cards. In oth r ords, th cr dit card issu rs r co r th ir costs from fraud b charging th m rchants a p rc ntag on th ir custom rs' purchas s. or this r ason this f is ariabl , and is much high r for, sa , Int rn t or t l phon purchas s than it is for purchas s h r th ph sical card is pr s nt d. It also ari s b industr s ctor, ith c rtain high-fraud busin ss s b ing p nali d ith high r f s.
  In short, th main r ason for th s high f s is th ins curit of th original cr dit card d sign, hich allo s m rchants to i (and cop , and r us) all of th custom r's pri at information.
  s a r sult of th s high f s, pa m nts of l ss than $ cannot b mad ith cr dit cards ith a r asonabl profit b ing mad b th m rchants (sp ciall for on-lin m rchants, ho incur high r charg s). ggr gating small pa m nts into on r asonabl si d amount b for charging on 's cr dit card is th solution curr ntl us d, but this pos s too man unn c ssar r strictions on both us rs and m rchants.
- **purc as s ar trac ab .** spit th con ni nc of a full histor of on 's purchas s, as ll as th abilit to disput pa m nts mad ith a cr dit card (sp ciall in th U), th fact that cr dit card issu rs ha all th us rs' sp nding information a ailabl pos s s rious pri ac conc rns. his information is sold to ad rtis rs, and is utili d int rnall b cr dit card issu rs to targ t ad rtis m nts to th ir audi nc . rom both an thical as ll as a practical p rsp cti , gi ing som on th abilit to conduct pa m nts should not go hand-in-hand ith kno ing th ir h r abouts, th ir sp nding patt rns, and th ir p rsonal pr f r nc s.
- **curit pr b s f r t cust rs.** On of th bigg r probl ms ith cr dit card pa m nts is that all th us r's pri at information is pos d to th m rchants. his allo s m rchants to ff cti l st al and us th ir custom rs' cr dit cards. Ob iousl , this is a much gr at r thr at o r th Int rn t, h r th m rchant can b locat d an h r in th orld.
  his s curit probl m is manif st d in t o diff r nt a s, d p nding on h r th cr dit card has b n issu d:
  - or cr dit cards issu d outsid th U , th nd-custom r is h ld liabl for all purchas s. hus, a stol n cr dit card numb r has a dir ct impact on th consum r. l arl , this is a s rious s curit probl m, sp ciall sinc th custom rs ha littl or no control hatso r o r th m rchants' handling of th ir cr dit card information.

– or U -issu d cr dit cards, th r is a r gulator limit of $5 on th consum r's liabilit in cas of a lost or stol n card numb r. In addition, most cr dit cards ill t picall r fund th hol amount from a fraudul nt purchas , so mor lik l than not th custom r's liabilit is nil. r dit card issu rs oft n tak ad antag of th fact that consum rs ar afraid of losing th ir cr dit cards b off ring th m additional "s curit guard" f atur s. In ss nc , this is an insuranc against th ft or loss of on 's cr dit card; th probl m is that th f for this insuranc is tr m l high, t picall .5 to % of th custom r's purchas s.

hus, in ith r cas consum rs ar unfairl p nali d for th cr dit cards' o n inappropriat s curit d sign.

3 lec r ic ec s

ollo ing th mod l of ph sical pa m nts, h r cr dit cards, cash, and ch cks combin to dominat th mark t, a logical st p for pa m nts ar l ctronic ch cks. scrib d in an abstract fashion, th s ar s qu nc s of bits that ncod a alu , and using ith r digital signatur s or oth r cr ptographic constructions allo s a r c i r to distinguish b t n alid and in alid bit s qu nc s.

om m thods ha ind d b n put to practic , but th r has b n no larg -scal adoption to dat . h bigg st missing link for th s sch m s is to put in plac l gislation go rning th us of digital signatur s and oth r cr ptographic functions, so that th t p s of digital agr m nts hich can b s n as binding can b d t rmin d. his is th r for an adaptation of th int rpr tation of ho ritt n signatur s ar binding. n though digital signatur s ha b n put to practic man ars ago, and n though th ar much hard r to forg than hand ritt n signatur s, th ar not t l gall binding to th sam t nt that hand ritt n signatur s ar (c pt in plac s h r la s r put in plac). his point cr at s a s r probl m for issuing banks: lack of a cl ar r gulation fram ork.

On of th larg st compon nts in th cost of ch cks is th ph sical d li r into and out of th cl aring hous s. tt mpts to mimic ch cks l ctronicall b pr s nting an l ctronic imag of ch cks caus s a larg traffic o r l ctronic n t orks, so it sol s th cost probl m onl partiall (h r as digital signatur bas d ch cks ha th pot ntial for b ing much ch ap r to impl m nt).

o, hil b li that "ch ck bas d" pa m nts ar iabl , and that th ill turn out to b important onc th ar succ ssfull introduc d, this is not lik l to occur b for mor sp cific l gislati structur s ar in plac . imilarl , th s pa m nt m thods d p nd on a compr h nsi public k infrastructur to b in plac b for th can b com common and id spr ad. Whil this is on th a of happ ning, it has not mat riali d t.

It is important to not that banks and financial institutions ar r lati l cons r ati du to th h a il r gulat d natur of th ir industr . h r for , -pa m nt impl m ntations to dat ar a r clos r fl ction of pa m nts in th ph sical orld, and do not incorporat f atur s that ould normall com

to mind in an l ctronic sc nario. or ampl , th r is no r al-tim cl aring m thod for l ctronic ch cks, hich although impractical in th ph sical-ch ck orld ould mak p rf ct s ns l ctronicall . On possibl r ason for this is that banks ha built th ir busin ss mod ls around a particular a of handling ch cks, hich ould b in alidat d ith th a ailabilit of r al-tim cl aring. Ho r, as t chnolog progr ss s th banks ill ha to catch up or th ar at risk of b ing b pass d.

pes f s -li e c e es

In this s ction, ill discuss som diff r nt t p s of cr ptographicall bas d pa m nt sch m s, broadl r f rr d to as " -cash" or "cash-lik " sch m s. his cat gori ation is n c ssar du to th multitud of propos d s st ms and th diff r nc s b t n th ir approach s.

4. at g ri i g b ri ac ti s

s highlight d in s ction 2, consum r pri ac is a major conc rn, consid ring th as ith hich data mining can b p rform d l ctronicall . h r for , a significant portion of l ctronic pa m nt s st ms afford som l l of consum r pri ac . W bri fl outlin th l ls of a ailabl pri ac in this s ction.

c s it rf ct ri ac . Information hich can b consid r d p r-sonal can b gath r d at s ral stag s in a pa m nt proc ss. o b gin ith, for r Int rn t conn ction th I addr ss of th consum r is pos d; this can b us d for arious t p s of tracing and is c rtainl pri at information. On th oth r nd, th m rchant ma plicitl r qu st p rsonal us r information in ord r to compl t a purchas . l arl , a pa m nt m chanism cannot d al ith th s "out of band" information l aks. h r for in our cont t "p rf ct pri ac " m ans that th pa m nt m chanism its lf hid s all consum r-sp cific information.

rf ct pri ac , fr qu ntl also r f rr d to as "us r anon mit " can b achi - d in man a s. non mit ma b stablish d at th tim of acquisition of som t p of b ar r instrum nt, similar to th a ph sical cash pro id anon -mit . Or, anon mit ma b stablish d at th tim of pa m nt, ith th us of cr ptographic t chniqu s; in this cas , th consum r can "con inc " a m rchant that th pa m nt information suppli d is corr ct, ithout r aling an infor-mation that could link this pa m nt to th acquisition proc ss, and th r for h r/his id ntit . h s t p s of t chniqu s ar call d " ro-kno l dg proofs". rom a cr ptographic p rsp cti , th s r th initial sch m s (bas d on off-lin coins) and th r bas d on "blind signatur t chniqu s" hich is mor ffici nt than g n ric ro-kno l dg proofs. h notion as put forth b haum [2] ho has b n for man ars a major propon nt of digital cash ithin th cr ptographic communit . h notion has b n in stigat d in th initial pap rs in th cr ptographic lit ratur [,OO 9,OO9 , Y93, 93, 93,O95].

c s it kab ri ac . ri ac , no matt r ho d sirabl , ma caus probl ms in th r gulator and l gal l ls. In particular sinc a b ar r instrum nt is, b d finition, alid for pa m nts in an op n n ironm nt, th r ists th pot ntial for mon laund ring, bu ing ill gal goods, blackmailing, and oth r attacks [92]. o pr nt against th s , som anon mous s st ms allo an administrati part or a coll ction of parti s to r ok th consum r's anon mit und r c rtain circumstanc s, such as a court ord r. uch r ocation is usuall mad possibl b forcing th consum r to ncr pt th ir pri at information und r th k (s) of th administrati authorit (i s). Wh n r ocation is ord r d, th ncr pt d data ar gi n to th authorit (i s) hich can th n d cr pt to obtain th consum r's id ntit . n alt rnati to r ocation hich has b n r c ntl propos d, is public auditing fil of coins and acc ss to r ok d coins ithin this cont t.

c s it ut ri ac r it i it ri ac c a is s. h r ar also s st ms hich do not mplo anon mit , usuall in th int r st of simplicit . spit th ob ious consum r ad antag of th a ailabilit of p rsonali d disput m chanism, compl t lack of anon mit usuall limits consum r app al.

hus, som s st ms mplo a mid- a for pri ac . Usuall this is p rform d b th ntit issuing th b ar r instrum nt (th "bank") poss ssing th consum r's pri at information, but pr nting disclosur to third parti s, including m rchants. om of th s t p s of sch m s ar fr qu ntl confus d ith "p rf ct pri ac " sch m s, but th fact r mains that th bank can still p rform data mining on us rs' p rsonal information; furth rmor , th bank th most lik l part to p rform such mining an a , sinc it poss ss s th larg st databas of custom r data.

4.2 at g ri i g b i f a t

In principl , a pa m nt m chanism should b abl to handl arbitrar si pa m nts. Ho r, th r ar t chnical as ll as r gulator r asons hich pr nt a singl sch m from co ring all possibl pa m nt t p s.

c s f r arg a iu a ts. n rall h n a larg singl pa m nt is in ol d th r ist r gulator r quir m nts to r cord th pa m nt amounts, or pot ntiall to allo disput of pa m nts. ut n in th abs nc of r gulation, consum rs ar unlik l to us a pa m nt m chanism for larg or m dium alu pa m nts if th cannot (a) asil obtain transaction r cords and disput pa m nts, (b) b assur d that th s curit of th m chanism is ad quat to prot ct th transmitt d funds. On th oth r hand, proc ssing costs, as ll as th tim to compl t a purchas , ar of l ss r importanc , sinc larg pa m nts ar conduct d ith r lati l small fr qu nc from th consum r's sid . lso, anon mit is of l ss r importanc , sinc a pa m nt trail is usuall d sirabl b th (la ful) consum rs to allo for transaction r cords and pot ntial disput s.

c s f r a a ts. In contrast to th r quir m nts for larg pa m nts, th prioriti s for sch m s that can b us d ith small pa m nt d - nominations ar (a) ffici nc , (b) anon mit , and (c) simplicit . ccountabilit , r cording of transactions and disput r solution ar of l ss r importanc – c pt for h n pa m nts ar aggr gat d to larg r amounts, but this can b s n as a form of a larg pa m nt and tr at d accordingl . o this ff ct, a sp cial cat - gor of sch m s has b n d lop d, traditionall call d "micropa m nts" sinc th allo pa m nts as lo as c nts or fractions of c nts. It is important to not that th micropa m nt computational cost cannot b too larg and r sourc con- suming (hich ould incr as th ir cost and ill d f at th ir purpos). hus, t chnolog lik blind signatur s, hich could ha pro id d anon mit for small pa m nts, is not us ful du to its computational cost.

4. i g s f a ss (r babi istic c s)

In th majorit of cas s, pa m nt m chanisms mplo d t rministic t chniqu s during th pa m nt rification proc ss. his t p of assuranc s ar traditional in th banking industr . Ho r, th r ar s st ms hich can obtain (computa- tional and oth r is) ffici nc ad antag s b p rforming som pa m nt-r lat d functions in a probabilistic a , thus spr ading th ff cti "cost" of an op ra- tion throughout multipl transactions and cons qu ntl achi ing high r o rall ffici nc .

H r d scrib s st ms in hich consum rs pa according to a probabilistic mod l, ith r honor-bas d (ou ha to pa ach tim , and if ou ar caught not pa ing in a random "ch ck" ou ar charg d a multipl of th purchas pric), or lott r bas d (ou onl pa infr qu ntl , but ou pa multipl tim s th purchas amount). om ampl s of such sch m s ar :

- **r babi istic i g.** h id a b hind probabilistic polling construction is to int grat a probabilistic function d fining th fr qu nc for s nding pa m nt to th bank. h s sch m s propos a probabilistic d posit at th tim of th transaction, corr lating th risk of o rsp nding to th fr qu nc of on-lin rification of pa m nts. ra backs of th m thod ar th n d for on-lin rification of us rs sol abilit and black-listing (hich r quir s to maintain black-list and k p inform d ndors of an n r ok d us r).
- **r babi istic u iti g.** In this s tting, a hard ar -bas d d t rministic sch m is combin d ith a probabilistic auditing of sp nding r cords (to d t ct o rsp nding).
- **r babi istic a i g.** h id a is to l t us rs s nd bids and pick ran- doml a transaction as a "contract" (or s ral transactions d p nding on th sch m s tting) that is (ar) d clar d as pa m nts. h us r committ d to th contract must finali th transaction and actuall pa th m rchant.

4.4 at g ri i g b I p tati atf r s

ar ar bas c s. an sch m s r l to som t nt on hard ar impl m ntations and assumptions. h s sch m s ar of t o major t p s:

– **curit r i s ar ar .** om sch m s, such as [on], d ri th ir s curit ntir l from th hard ar us d. In [on], us rs carr hard ar , and in th hard ar a stat corr sponding to th balanc k pt. Wh n a transaction is p rform d, this balanc is alt r d corr spondingl . l arl , such a sch m ould not b a good id a if impl m nt d in soft ar , as it ould allo us rs to ith r incr as th ir balanc b incr asing th count r, or n simpl r, b "r inding" to a pr ious stat aft r a pa m nt is p r-form d. In sch m s lik th abo , a probabilistic approach can b mplo d to limit th cost of th ch ck, b onl p rforming on-lin rification for a c rtain fraction of th transactions, as discuss d abo .
– **curit i pr b ar ar .** In oth r sch m s, such as off-lin coin-bas d sch m s, th hard ar is us d to pr nt o rsp nding. n though th s sch m s ha m chanisms in plac to d t ct and trac o rsp nding, and som sch m s allo th bank to block oth r coins issu d to th fraudul nt us r, th us of hard ar can r duc th amount of litigation, blacklisting, and complicat d cas s in ol ing mor than on countr .

ft ar - sc s. h r ar man propos d sch m s that do not r l on hard ar . o diff r nt cat gori s can asil b distinguish d:

– **rau is pr tab .** In on-lin sch m s (for a clarifi d ampl s [96]) th bank or a cl aring ag nc g ts in ol d in r transaction, and rifi s that funds ar a ailabl . It is th r for possibl for th bank to asc rtain that nobod sp nds funds h /sh is not ntitl d to. h bank can rif that a us r is ntitl d to sp nd an amount ith r b rif ing that h has a coin (or similar) b aring a alid signatur , and also rif ing that this coin has not b n pr iousl sp nt. lt rnati l , th transaction ma b account-bas d, allo ing us rs onl to acc ss funds b id ntif ing th ms l s as ha ing acc ss to an account that th bank k ps. In th latt r cas , th bank d t rmin s th pr s nc of th account, as oppos d to th abs nc of a pr iousl sp nt coin ith th lab l in qu stion. oth of th s approach s ha th dra back of th slo do n of th transaction du to th onlin conn ction ith th bank, and th incr as d cost du to on-lin a ailabilit r quir m nts.
– **rau is u pr tab .** In micro-pa m nt sch m s, ach unit of funds is so small that th r is no significant risk of fraud, as th amount to b gain d is not substantial. lso, this t p of pa m nt sch m is lik l onl to b us d in situations h r th r is no cl ar b n fit associat d ith a tr m ndous o rsp nding (such as acc ss to hom pag s, tc.). It is important to d sign th supporting archit ctur to pr nt accumulation of ast amounts of small pa m nts to b us d for som thing of high alu that can b d li r d b for th bank d t cts o rsp nding. (his t p of d la is an important but littl studi d tool for r ducing th inc nti of misb ha ior.)

4. at g ri i g b t I frastructur

bas . p ciali d compani s ha b n proposing to pa for transac-tions b charging th s to th pa r's phon bill. In principl , an bill could b

us d for this, .g., th gas and l ctric bill, but it mak s mor s ns to charg purchas s to th phon bill, as in man cas s th phon ould alr ad b in ol d in p rforming th transaction as ll.

I t r t bas . h n t a of pa m nt sch m s int grating pri ac pro- t ction, non-r pudiation f atur s and nlarging th custom r bas of l ctronic comm rc is ob iousl bas d on th Int rn t r olution. Ind d th Int rn t is th n ar na for comm rc and man oth r human acti iti s. h ampl s of -comm rc s r ic s lik ama on.com or a d monstrat th impact and pot ntial of th Int rn t cont t on old busin ss and trad mod ls. h n s tting nabl s an custom r to choos and d cid kno ing b tt r and b tt r th r lati alu of goods and s r ic s. Oth r mod ls of busin ss ar dir ct and oth r comput r quipm nt purchasing. h s sho anoth r no l busin ss mod l that th Int rn t nabl s. h dir ct acc ss to custom rs and r duction of suppl chains ithin and b t n organi ations ar p ct d to furth r n- hanc th conomic alu of th Int rn t. Ho r, risks and probl ms of this n m dium ist as ll [aYu9]. W b li that it is quit an acc ptabl pr diction to d clar that d dicat d pa m nt s st ms ithin th Int rn t ar na ar of prim importanc .

ples f c e es

Will ill no m ntion a f sch m s, cat gori th m gi n th abo pa m nt sch m ta onom , and bri fl discuss hat t p s of situations th app ar to b b st suit d for.

. r it ar tti g a - i c s

- **t i :** his sch m [95] is bas d on th on-lin paradigm using ba- sic auth ntication m thods. h ork includ som no l int r sting f atur s such as atomicit of pa m nts (a fault tol ranc f atur h r b a us r pa s onl for transactions h r c i s) and anon mit b usag of ps udon ms. h dra backs ma b th numb r of m ssag s ( )to proc ss for a tran- saction, and th mandator on-lin communication ith th int rm diar NetBill s r r. W comm nt that th issu of fault tol ranc rais d b th atomicit conc rn is r al and important in d plo d s st ms (s also [94, H Y96, 96, W97,XYZZ99]).
- **t qu a t as :** his proj ct [95] manag d b th Uni r- sit of outh rn alifornia is anoth r on-lin sch m h r us rs issu ch cks using a s cr t k (shar d b t n a us r and th bank) as a c rtificat of alidit . akn ss ma b th n d of us rs to r gist r at th banks, and th on-lin rification of ch ck corr ctn ss and fund a ailabilit hich is r quir d for ach pa m nt. Off-lin rification is a t chnical possibilit , but at th cost of possibl fraud (non-d t ction of bad ch cks). his proj ct is an t nsion of NetCash [94] hich impl m nt d l ctronic curr nc in

a a som hat similar to th igicash sch m . Ho r, th t h qu s st m onl k ps track of tok ns in circulation, i. ., thos issu d but not alr ad sp nt.

– **:** I and 's analog to a cr dit-card s tting hich incorporat s l gall -binding signatur s, and impl m nts digital signatur s as a tool for auth nticating us rs, m rchants, and banks. his r duc s th possibilit of fraudul nt transactions, thus bringing on-lin transactions on par ith ph sical-card solutions. h t chnical d tails, originat d b t chnolog compani s: I , icrosoft and tscap orking tog th r ith th cr dit card compani s, ar solid. ot ho r, that th compl it of has, so far, hamp r d its full-scal d plo m nt. It is, in fact, too p nsi for most m rchants to impl m nt, and it also r quir s nd-us rs to do nload sp cific soft ar and to participat in a public k infrastructur – hich is not t firml in plac . lso, n do s not rais cr dit cards to a suffici ntl high s curit standard to compl t l o rcom fraud, h nc cr dit cards still charg m rchant f s hich mak s micropa m nts prohibiti .

– **igi as :** h igicash pa m nt sch m in ol d so-call d blind signatur s, hich ar standard signatur s g n rat d in a mann r that do s not allo th sign r to l arn th m ssag or th actual signatur , but onl th ir g n ral format. his is don in a ithdra al phas , nabling th ntit to lat r b com th pa r ho holds a signatur b th bank. h n, in a pa m nt phas , th pa r s nds this signatur to th m rchant, ho for ards it to th bank. inc th signatur as ithdra n in a blind d fashion, th bank cannot d t rmin hat ithdra al s ssion it b longs to, but onl that it is a alid signatur . Upon s ing such a alid signatur , th bank rifi s that it has not b n d posit d alr ad , and ackno l dg s th transaction to th m rchant if this has not tak n plac . lat d rsions allo ing off-lin purchas s ha b n d lop d – th s , ho r, r not impl m nt d du to th risk of short-t rm high- olum o rsp nding, hil b ing computationall int nsi (as oppos d to micropa m nts, b lo). h igicash on-lin sch m has b n impl m nt d on arious platforms. for th nd of igi ash op ration, thr smart-card bas d rsions, th so-call d igi ash lu ask, ist d. h s sch m s ar clos r to hard ar -prot ct d micropa m nts. h larg r of th s rsions (K O , K O and 256) impl m nt d hat is kno n as th optimal ast bit command ith compr ssion, nabling man fast pa m nts for transaction tim around 2 ms.

.2 r babi istic a t c s

Whil most sch m s ar d t rministic in th a th tr at l galit of pa m nts, a f probabilistic m thods ha b n discuss d.

– **i g c s :** abb r and ilb rschat [96] and ar cki and Od l ko [O97], propos d sch m s h r :

. us rs r gist r b gi ing a first pa m nt, hich is a sign d not including a bank c rtificat ;
2. subs qu nt pa m nts s nt b us rs (d p nding on th und rl ing pa m- nt sch m) ar r c i d b th ndor and probabilisticall s nt to th bank for d posit at th tim of th transaction.

h o rsp nding risk can b limit d to a kno n alu b d fining th probabilistic ch cking as a function of th transaction si (making larg pa m nts mor lik l to b ch ck d.)

– **Yac bi's u iti g c** : In [Yac97] a hard ar -bas d d t rministic sch m ith a probabilistic auditing of sp nding r cords (to d t ct o rsp n- ding) is propos d. his proj ct at icrosoft s arch includ s th follo ing f atur s:
  – smart-card id-bas d all t (tamp r-r sistant d ic)
  – -coins sign d b th bank and stor d in th smart-card
  – duplication (doubl -sp nding pr ntion) controll d b probabilistic ch cking in th d ic

– **i st's tt r** : In this lott r bas d sch m [i 97a], th id a is to us a chain of alu s as a book of lott r tick ts. h us r pa s ith th n t alu (or pr -imag) in th book (as ill b d scrib d in th coupon s ction 5.5) but ith th t ist that th bank lat r announc s on of th tick ts as a inning tick t. If th us r sp nt th corr sponding tick t, th n h is r sponsibl for pa ing th ndor ith th tick t alu . h lott r must b h ld aft r th book (of th da , of th k) is not in us an mor , to pr nt ch ating us rs from tr ing to n r sp nd a inning tick t.
In a ariation of th sch m in [i 97b], th d cision to p rform a pa m nt is don b both th pa r and m rchant ho cut a standard coin-flipping protocol (m rchant commits to a random numb r, pa r s nds a gu ss and ndor d -commits) to d cid jointl if th us r should pa or not.

. ar ar as c s

– **a a u a ts :** t rn and aud na 's sch m [97] propos d to d li r to ach ndor a smart-card containing a mast r k . Us rs bu tok ns c rtifi d b th bank using th pri at -k sch m ; th p rform a pa m nt b s nding a tok n to th ndor's d ic hich ch cks th c rtificat in ord r to alidat th transaction. h id a is that onl th bank kno s th s cr t k hil an ndor can rif prop rl th tag auth nticit . h main s curit issu is r lat d of th mast r k storag on ach indi idual card sinc br aking a card is qui al nt to g tting th sch m 's mast r k .

– **icr - i t :** i st and hamir [96] propos d a sch m in hich man collisions ar found b (substantial) pr computation b th bank; and such collisions ar hand d out to us rs lat r. collision, hich is hard to find for us rs, th r b b com s th tok ns us d for comm rc , much lik pr cious m tals for a long tim r us d for coins. h principl of th sch m is that h r as a lo numb r of collisions is hard to find, a larg numb r of

collisions is not r r to find, th r b allo ing amorti ation. thods for distributing th ffort of finding collisions r r c ntl introduc d in [99].

– **bri c s :** h ad antag of ha ing a unifi d sch m hich orks in soft ar and hard ar (assuming card r ad r/ rit r in th) is ad o- cat d in [Y9]. h sch m combin s soft ar bas d (on-lin) sch m hich is s nchroni d ith a smartcard bas d sch m h r loading can b don ia th n t ork.

.4 as a t

– **a :** his anadian compan [l] propos s a pa m nt-b -phon s r ic to r gist r d custom rs. uring r gistration, ach us r is gi n a uniqu r gistration numb r associat d ith a p rsonal id ntification numb r (I). Onc s t up ith a r gistration numb r and I , it is n c ssar to also s t up th accounts us rs ish to pa . his r quir s id ntif ing th pa (compan to b paid) and nt ring an account numb r ith that pa . his information is ch ck d b l a s st m to nsur , as far as possibl , that it is alid. rom th n on, to mak a pa m nt to that account all that is r quir d is that us rs dial th last thr digits of th account numb r. h amount is nt r d and th s st m, hich confirms th nam of th pa and amount to b paid. n us r can modif his profil and nt r additional d tails ith r r garding bills alr ad r gist r d or n bills to app nd to th list of pa s.

– **ibi / arg :**
o r c nt s r ic s, ibill [ibill] and harg [harg], also allo m rchants to charg transactions to th phon bills of th pa r, but in a slightl mor str amlin d mann r. Wh r as ibill focus s on th adult mark t, and parti- cularl subscriptions, harg pr ssl clud s this mark t. oth us a conc pt clos l r lat d to 9 numb rs, r quiring a phon call b th pa r to b mad in ord r for th fund transf r to occur. In ibill, this in ol s th us r manuall , h r as in th sch m b harg it is don ia a mod m. oth of th s s r ic s allo onl fi d charg s of a small ari t of d nominations, and so, do not allo for shopping cart t p of purchas s. n ad antag of this t p of s r ic is that it is as for th a rag consum r to us and und rstand; a dra back is that it r quir s th phon s r ic pro id r to ac- c pt th risks in ol d in th t p s of purchas s in ol d, hich is outsid th t pical busin ss mod l of th s compani s.

. up -bas c s

– **a p rt -ti -pass r bas sc s :** arious sch m s r l on an id a from amport: i st and hamir's PAYWORD [96], nd rson's t al. NETCARD [96], d rs n's ch m [d95], utla and Yung's PAY- TREE [Y96b] and Haus r's t al. MICRO-IKP [H W96]. h id a is th

follo ing : tak a on - a p rmutation f (or a hash function), pick a random input x and it rat th application of f a larg numb r n of tim s to produc $y = f\ (x) = f(f..(f(x)))$ and auth nticat y ith a public-k signatur sch m . h chain of alu s $y, f^{-}\ (x), f^{-}\ (f^{-}\ (x)), ...x$ has th prop rt that gi n an l m nt of th chain, it is hard to comput th pr - imag (du to th on - a n ss prop rt) but as to rif that this chain l ads to , auth nticat d b th bank. h g n ral construction of a pa m- nt sch m bas d on this id a is to d li r to us rs tripl s of th form $(x, y,$ sign$(y))$; h n us rs ant to pa , th sp nd an in rs as a micro-pa m nt unit. utla and Yung g n rali d th chain id a to tr s. h dra back is again th doubl -sp nding attack; pr ntion against this attack is to ch ck on-lin (hich is p nsi) or to blacklist mal ol nt us rs (but th us r's id ntit must b prop rl built in, so that forging/changing th id ntit is hard to do).

– **-c u t r t c :**
h -count protocol d sign d b th compan chnolog [qct] is bas d on th chain alu id a. h card contains a k ind k and th t rminal a -count r d not d x . h pa m nt protocol int grat s th follo ing st ps:
 . ard s nds th k ind k to th rminal
 2. rminal r pli s ith th follo ing data:
   – chain param t rs (N, TID, CID, u)
   – amount to b paid m
   – curr nt count r alu $(x\ )$
 3. ard comput s $x\ = G(S\ , TID, CID, N, u)$ and $x\ , x\ , \ldots, x\ _{-}$ h r $x\ = F\ (x\ )$
 4. ard comput s $x\ _{-}$ and d cr as s balanc b alu $m * u$
 5. rminal ch cks if $F\ \ (x\ _{-}\ \ ) = x$

S is a s cr t k , F and G t o on - a functions. h l ngth of th chain d p nds on th natur of sp nding. h sp nding of mon on th road can b don in a location ith a b acon or b t n t o b acons. t o b acon s tting gi s nough tim to pr par th transaction (b t n th r adings), th tim r quir m nt b ing l ss critical. On th contrar , in a on b acon situation, th total transaction must b proc ss d in l ss than 2 ms. In this cas , th chain is minimal (l ngth) and th mpt -count r at t rminal is $x\ = F(x\ )$. h card ill simpl comput and s nd x .

– **i i t :** igital (curr ntl ompaq) s arch sch m MILICENT [95] is a pri at -k solution h r brok rs, conn ct d to a c rtain subs t of ndors, ar in charg of s lling -coins r lat d to a ndor. h s ndor-sp cific coins can onl b auth nticat d b th ndor, using his pri- at k . h brok rs must b trust d and ha agr m nts ith ndors (c rtification). his sch m is on of th initial micropa m nt sch m s.

.6 c s it kabi it

h anon mit coming ith th unr strict d usag of blind signatur m chanisms could l ad to attacks from larg -scal criminal organi ations. In ord r to

r duc such risks and impro control and r liabilit of anon mous pa m nt sch m s, th conc pt of r ocabl pri ac as introduc d. In such a s tting, pri- ac can b r mo d to id ntif mal ol nt us rs or trac improp rl ithdra n coins. scro d cash sch m introduc d in [92] as sch m s bas d on th fair blind signatur primiti [95] gi a good fla or of th conc pt but r qui- r d th rust s to g t in ol d during ithdra als (also [K95]), d cr asing drasticall o rall p rformanc of th sch m . c nt orks introduc d th first r ocabl off-lin (.r.t to th rust s) sch m s, bas d on publicl rifiabl s cr t sharing t chniqu s [96, ta96] or on indir ct discours proofs [Y96] (s also [Y97,d 9 , Y9]).

n int r sting mod l from akobsson and Yung [Y96a] introduc d th no- tion of Ombudsman (a go rnm nt official in charg of th custom rs d f ns against abus s) i lding an ffici nt l ctronic mon s st m h r tracing do s not onl d p nd on th bank but r quir s th combin d nd a ors of th bank and th Ombudsman in th tracing proc ss. urth rmor , th pap r introduc d n t p of attacks, including bank robb r attack corr sponding to an ad rs- ar abl to acc ss to s cr t pi c s of information, and a s of prot cting us rs and issu rs against th s .

ral impl m ntations such as [96] bas d on th fair blind signatur primiti or [' 96], sub-contracting th blinding to a trust and using an Id ntit -bas d pi c of information to achi pro abl pri ac and s curit , r p rform d on smart-cards, pro ing th practical alidit of such conc pts.

ch m s bas d on public auditing for crim pr ntion rath r than r ocation r gi n in [99a, 99b].

6 ec l si ess/ li ic l ss es

In ord r to app al to mainstr am custom rs, ha larg m rchant bas , and g t man in ol d in th pa m nt s st ms, t chnolog and oth r factors: busin ss, l gal, polic and political on s ha to b r concil d. Whil th richn ss of a ai- labl sch m s is justifi d t chnicall (and has to b pursu d b sci ntists), th mainstr am solutions ha to account for man conc rns. h int gration of th solutions, sp ciall th global larg scal on r quir s a lot of und rstanding of th r gulator , financial, social and oth r asp cts of th us r bas (cli nts, m rchants, financial institut s (old and n), go rnm nts, r gions and global mark ts).

Int grating pa m nt t chnolog ith oth r t chnologi s (fault tol ranc , dis- tribut d s st ms, Int rn t int rfac s/ I's, oth r -comm rc infrastructur , tc.) is still chall nging sinc cr ptograph is m r l a compon nt of th ntir s st m. om op n issu s ar in [97,W9].

What is int r sting to not is that man of th issu s d alt ith b th t ch- nical communit ar also issu s pr ss d in th busin ss orld (som tim s aft r th r r cogni d t chnicall). an of th t chnical conc rns in th cr p- tographic lit ratur r i d so far, ind d, ha parall ls in th busin ss, l gal and polic lit ratur . h banking industr has r port d conc rns r gar-

ding count rf iting on th us r sid [a96, a97a] and risk sup r ision a oiding commitm nts to unback d funds on th bank sid [a97b, a9]. an of th conc rns r garding mon laund ring is pr ss d in num rous polic ork, .g. in [96, O9 , W9 ,O 96]. ossibl l gal probl ms ith anon mit ar pr ss d in [95].

Ho r, larg scal studi s of compr h nsi t chnological solution ha not b n don t. h issu of conomic stabilit assuranc s that n curr nci s should maintain (t chnicall and oth r is) is an important issu . h d - lopm nt of stabl and ll r cogni d busin ss mod ls ill h lp in int grating op rational pa m nt sch m s into th busin ss orld. h issu of ducation of th us r bas , mark t(s) p n tration and th o rall int gration of pa m nts as an infrastructur compon nt ith m rging -comm rc applications is an int - r sting chall ng . h d p nd nci s b t n th gro th of comm rc in cont nt, consum r habits and th n d for -cash ha to b b tt r und rstood as ll.

r c nt int r sting anal sis of som of th r asons for th initial busin- ss failur s of micropa m nts is pr s nt d in [ro99]. H also tri s to plain h a curr nt tr nd of r rs micropa m nts (from compani s to consum rs as r ards for r ading ad rtis m nt or participating in som acti it) ma b mor succ ssful at th mom nt.

7 re irec i s

In this s ction, ill bri fl tr at som pot ntial sc narios, and discuss hat pot ntial constraints/ implications th ma ha on -comm rc . th na- tur of th discussion, it is impossibl to b hausti in this pos , and focus onl on a f pot ntial nts, and do not consid r th implication of combinations or t nsions of th s .

7. ga stricti s i a cia r pt grap ”

In light of th curr nt d bat , it is not unlik l that som countri s ill impos r strictions on th t p of cr ptograph us d b th ir citi ns. urr ntl such limitations ar on bulk ncr ption and ar s t from national s curit p rsp cti . Ho r, this ma chang ith th lik l gro th of -comm rc in t rms of its impact on local conomi s. In this cas , th flo of mon b com s as important to control as th flo of information (r call th abo polic pap rs m ntioning thr ats of -cash). h r for , n if pa m nt sch m s ar not asil abus d for us for s cr t communication, local go rnm nts ar lik l to ant to control th flo of s r ic s and funds, much in th s ns of hat customs do s for its ph sical count rpart. his d sir ma furth r limit hat kinds of pa m nt sch m s ar mplo d, and ma , for ampl , forc pri ac to b com mor of a l gislati m asur than a t chnical m asur . lt rnati l , it ma cr at mark ts for local pa m nt sch m s (for hich us rs njo pri ac , but ta s ar automaticall charg d b th local go rnm nt as a part of an transaction), and global sch m s mainl mplo d for chang of curr nci s b t n local sch m s. h s , in

turn, ould ork as th int rfac s b t n diff r nt l gislati and ta domains, and ould ha ta ation as a main obj cti . In such a situation, “black mark t” chang of funds ma b com a probl m much r s mbling hat pirac is toda , and ould ha to b battl d ith a combination of l gislati and t chnical m asur s.

noth r limitation ma pr nt or r strict c rtain t p s of cr ptographic tools to b mplo d, ith r globall or in particular countri s. his in its lf ma caus diff r nt sch m s to b mplo d, as ill local r quir m nts on th functionalit of th sch m s (som thing can alr ad itn ss toda ith th di ision b t n urop an cash cards and U. . cr dit cards.) isting cultural diff r nc s hich t pifi s ariations in ph sical pa m nt m thods ma migrat into th -pa m nt s st ms. dditionall , and as ill discuss in th n t subs ction, a multitud of diff r nt sch m s ma ol and b mplo d in th sam mark t.

7.2 a ara ta ar s

a m nt sch m s toda gi th impr ssion of b ing on th a of b coming a nich mark t in hich ha a f l ad rs for common t p s of pa m nts, and sp cial sch m s us d onl in particular situations. h r ar man r asons that such a ari t of sch m s ma b d plo d, ith r s mbioticall or in comp ti- tion ith ach oth r. h r asons ar ranging from corporat int r sts to ar ing r quir m nts on pa m nt sch m s bas d on th ir usag . On ampl of th s m- biotic us as gi n in th pr ious s ction, hil oth rs could aris to gi us rs b tt r functionalit , and to co r a ari t of situations. or ampl , fast and lo -o rh ad sch m s ar us ful for situations lik pa ing for dail commuting tolls, hil fr qu nt-fli r programs and th lik r quir no sp d of transactions, and ma put r strictions on ho funds ar transf rr d and us d (or ta d h n doing so). till, incorporating sch m s to allo for a consolidat d pr s ntation to th us r, and allo ing for (pot ntiall automatic) transf r possibiliti s gi ris to a much mor rsatil construction. Wh r as much of th probl m r maining to b sol d is that of building an appropriat infrastructur , it is also important to impl m nt m chanisms for monitoring (b la nforc m nt, customs, arbi- t rs, and oth rs). It is int r sting to notic th trad off b t n monitoring and pri ac h r , gi ing ris to a much mor s r pot ntial pri ac intrusion than hat has pr iousl b n consid r d.

7. a c s i r pta a sis

d anc s in cr ptanal sis ha th sam pot ntial as l gislation to chang th pa m nt sc n b limiting th allo d t p s of op rations. his ma r strict th us of c rtain sch m s or t p s of sch m s. It is not orth to point out that a ast majorit of pa m nt sch m s discuss d in th cr ptographic communit ar bas d on public k cr ptograph . In th unlik l nt of major cr ptanal tic br akthrough, a n approach ma b n d d. his, along ith conc rns of l gal r strictions, calls for car ful studi s on ho to impl m nt d sirabl pa m nt

sch m s r l ing on s cr t k cr ptograph or on oth r m thods or combination of m thods to nsur corr ctn ss of pa m nts.

7.4 cia a c ica a g s

l arl , social chang s can b p ct d to ha a major impact on th fi ld. or ampl , if 's b com as common as cr dit cards ar , it ill drasticall simplif th building of a n infrastructur for pa m nts. imilarl , t chnical chang s, such as a substantial incr as of th a ailabl communication band- idth (and th pric for it) ma aff ct hat t p s of sch m s ar mplo d. s an ampl , it mak s littl s ns to impl m nt off-lin pa m nt sch m s if th cost of communication drasticall falls, gi n th high r costs and compl it of such sch m s. h r is a tr nd to ards both of th s chang s. Ho r, at th sam tim as such chang s simplif th mplo m nt of pa m nt sch m s, th also incr as th s curit conc rns, as should b id nt from th ist nc of irus s. o far, th s ha not start d to surfac on 's, but such an nt is lik l to onl b a matt r of tim . ik is , du to th lack of l ctronic pa - m nt sch m s in common us , irus s ha not start d to targ t th all ts of us rs. his, too, ma simpl b a qu stion of tim . rom a t chnical point of i , that should prompt mor s cur op rating s st ms to b construct d for th s d ic s (or not r l ing compl t l and sol l on th computing platform), as ll as r co r m chanisms for pa m nt sch m s. h s ma b bas d on automatic arbitration, support d b tracing m chanisms and d t ction m cha- nisms controlling "unusual" flo patt rns. h latt r, in turn, forc s patt rn cat gori ation, hich ma b qu stionabl in t rms of pri ac conc rns if not p rform d b th us r hims lf, or mad non-int rpr tabl to a third part looking for diff r nc s in b ha ior.

cl si

W ha pr s nt d som of th past issu s ith th t chnolog of l ctronic pa m nts. his ar a is chall nging and promising. W b li that th n d for it is inh r nt, though th difficulti s in achi ing it ar t nsi and int rr - lat d to man mor g n ral -comm rc and s cur infrastructur issu s. W ha sur d som protot pical ampl s from th past and th pr s nt. W cat gori d th t chnical solutions. W furth r r lat d th t chnolog to man non-t chnological constraints and discuss d possibl futur n ds, dir ctions and possibiliti s. Whil could not ha possibl co r all ar as and s st ms in this r prolific fi ld, hop ha pr s nt d th basic t chnological d lop- m nts (grant d, ith unint ntional omissions!). W b li ha point d to arious int r sting and chall nging issu s for furth r acti iti s. h s acti iti s ar n d d in num rous ar as: r s arch, busin ss d lopm nt, t chnical r s arch and d lopm nt, social, l gal and political studi s and oth r int rdisciplinar ar as r lat d to -comm rc and pa m nt m chanisms.

efere ces

S R e , a fa a , a S he a e ca - a ac ca e ec c ca h e *rth m ridg rks- h c rit r t c ls* S ge - e ag, a ab e a http://www.cl.cam.ac.uk/users/rja14

a Re b he ee Pa e , Se e e S e , a he f e E e f e a a f he f Te c e , Se- c f E ec c e , h b g b e h ,

a a Re f he g a e ec c e f he f Te c - e , E ec c e - e P ec , a e f ce e , S e - a e e , h b g b e h ,

a b a e ee a g S e , e P c e f Effec e a g S e , h b g b e h ,

a 8 a e ee a g S e , R a age e f E ec c a g a E ec c e c e , h b g b e h , 8

S a , U aceab e ff- e a h a e h b e e ,

4 , e ae , R a e , R che e , S , e , T Pe e e , Pfi a , P e R , Sch a e , Sch e , a ee a a e , The ESPR T P ec E gh Sec D g a Pa e S e , ES R S 4

Y 8 e a e, a a , a, a Y g, *ri t sh* -P e E ec c Pa e S e E e e b ac , U e h E- ec c e ce 8

5 E c e , P e e , a D a , T ee- a e T ac g E e - a h a he a g f ha ge, S D 5

P8 a Pfi a , D g a Pa e S e E ab g Sec a U b e ab , e & Sec , 8 5, 8 , -4

8 D ha , S g a e f U aceab e Pa e , 8

88 D ha , a , a a , U aceab e E ec c a h, 88

T 8 ha , Y a e , a Y T , Ea e-Ea D b e a h, E c 8

TY a , a a , D T ga , a Yee, c T a - ac , U e E ec c e ce,

S a e ch, U a e , a S a e D g a Pa e S e h Pa e -Re g T ee *’ 6*, S 4 S ge - e ag,

PS 5 a e ch, - P e ea , a S a e a S g a e *r cr t ’* , S , age – S ge - e ag, 5

PS a e ch, - P e ea , a S a e Effic e a Pa e S e *r c. f th rd* , age 88– 4 e ,

TS 5 , D T ga , a S b e b ec a a ac c *irst rksh l ctr ic mm rc* , 5 a ab e a http://www.ini.cmu/NETBILL/home.html

S c e , The S e S g f e e c a e *i g i* , http://www.cisp.org/imp/april_99/04_99crocker.htm

D TY Da a, Y a e , Y T , a Y g, e-ca h he - a c a g a h , S 8 S ge

a b e a

ST 8 e S age a T a e, Effic e a ff- e e ec c ca h h e e chec a a e h b e e , he - a c a - g a h

e ha ge e ha ge, http://echarge.com

T T - e e a e g g e , a c a e E - f ce e e P b ca , h ea g fi ce b h ,

e g , E e f S g e-Te ,

Y 8 Y a e , D a T g e a Y g, e e a a -ba e D g a S g a e T a ac , *i ci l r t gr h*

TY Y a e , Y T , a Y g, ec D c e P f ch e g a ff- e E- a h, ac

TY 8 Y a e , Y T , a Y g a ff- e e- a h a e Ea , ac 8

Y a a Y g, Sec e a Effic e ff- e D g a e , P S , S ge e ag

5 , a E e , a f - e a , a 4

8 e e a cc g ffice , P a e a g Ra Sa a , ba , a ege e a e g, h ga g , 8

5 S a a , a a e, ba a , P a h e , a P S ba - a The ce P c f e e e E ec c e ce *rth t r ti l rld id f r c* , 5 a ab e a http:www.research.digital.com/SRC/milicent

S E abbe a S be cha g a a D b e P c f E ec c e ce *rksh l ctr ic mm rc* ,

S R a e , S e e , a a e c -Pa e ba e P *rld id gr ss m t r d mm ic ti- s c rit r t c l,* a ab e a http:/www.zurich.ibm.com/Technology/Security/publications/1996/HSW96-new.ps.gz

b b http://www.ibill.com

c Q ech g http://www.qctechnology.nl

5 a b , R g f a a E cha ge, E c 5

8 a b a D Ra h , -ba e E ec c Pa e , h Se ec e ea g a h , 8

Y a a b a Y g Re ab e a e a e E ec c e *r c. f th rd* , age –8 e ,

aY 8 a b a Y g a ce S c e f - e ce *i ci l r t gr h*

a b , e , P f f a ea g P c , S

S a ec a Effic e c a e Sche e ba e P bab c P g *i ci l r t gr h* ' , S 8 S ge - e ag,

Y b S a a Y g Pa T ee e -S g a e f e b e c Pa e *c d rksh l ctr ic mm rc* ,

4 e a e a e ca h De g f P ac ca E ec c e c he e e *c d f r c m t r d mm ic ti c rit* , 4

8 R a e , D g , a P , be a e a e a e g,
h a g b ca R R 5 R 5 f, 8 e http://www.mondex.com
R D Ra h -Effec e Pa e Sche e h P ac Reg a *si cr t ' 6*, S , age – 5 S ge - e ag,
5 e a a e Re e e f e Pa e The e che e P ec e , 5 a ab e a ftp://prospero.isi/edu/pub/papers/security/
E D ga a f Ec c - e a a De e e , E D - h he Ec c f he f a S c e ,
5 T a , Effic e D b e E ec c a h Sche e, 5
8 T a a h a, D ab e Ze - e ge he ca a The ca U aceab e E ec c a h, 8 T a a h a, U e a E ec c a h,
Pe 5 T Pe e e E ec c Pa e f S a Tech ca e , a h U e , e Sc e ce De a e , 5 D P -4 5
P Pfi a a a e , S g T e a ce f E ec c S e , T a e S e 5 , 4-
R a R R e E ec c e T c e a c - a h *i ci l r t - gr h '* , S 8 S ge - e ag,
R b R R e e T c e a c - a h, a c a g a h R Se
RS R R e , Sha , Pa a c T e c a e che e , a a e
ST a T Sa e a Ta-Sh a, e ach f E ec c a h S e , *i ci l r t gr h '*
ST b T Sa e a Ta-Sh a, ab e, E ec c a h E - e e b ac , *r t '*
S Sch e a e , a c Sec f he eca h Pa e S e , - e Sec a a g a h S a e f he a E , S e e ,
S D S , ca a a h, *r t ' 6*
S a S a e P b c e fiab e ec e ha g *r cr t ' 6*, S , age – S ge - e ag,
SP 5 S a e , P e ea , a a e ch, a S g a e, E - c 5
S S e a S a e a S a - a e a e a fle b e c a e che e *i ci l r t gr h '* , S 8 S ge - e ag,
T D T ga , c E ec c e ce, S P - c e f D b e g,
Te Te Pa http://www.telpay.ca
S S S a D accache S g a e a Pe fec e *m t rs & c rit* , 58 –58 ,
8 a e , e e Sec e E ec c e ce, 8
XYZZ S X , Y g, Zha g a Zh , e e a a c a ff- e E- a h ' a a , a a a, S ge - e ag,
Yac Y Yac b he c be ee - e a ff- e e-ca h e *i ci l r t gr h '* S ge - e ag,

i i- r l r i

og r K r, oac i os gga, a d Harald ogt

De che Te e , Tech g e e
T Sec Re ea ch F 4
D- 4 Da a
{Kehr|Posegga|VogtH}@tzd.telekom.de

c e e c be he Pe a a a , a ce a ha b g ge he PD a a ca The e g ea ha a PD ac a a e a e ce f c g a a ca a ache g a a e c e a
e e c be h ch a a ach ca be e f c ea g g a g- a e a c a , e ca c c e he b e e h e c e e e h c e
e c e ha f e f a c e e e f g he P a e h ca be e f eg a g he PD a a ca e ce e a b e e c f e h

r c i

r ptograp ca pro id s curit -s r ic s bas d o ll-fou d d at atics. k probl it appl i g cr ptograp to r al- orld probl s is, o r, t i t rfac to r al lif . I t is pap r i stigat a applicatio ar a r t is probl is r id t, i. .: t pr s tatio of a docu t t at is to b digitall sig d.

igital sig atur s for applicatio s lik l ctro ic co rc r quir ig s cu-rit sta dards. o cou tri s a alr ad propos d to b d digital sig atur s i to l gal fra orks, t ost pro i t a pl b i g t r a digital sig atur la " ig aturg s t " [,2]: is la r quir s (a o g ot r t i gs) t follo i g I s curit l ls for a s st us d for d ali g it digital sig atur s:

– storag co po t for t s cr t k (usuall a s artcard) ust t t crit ria of I 4 [3], a d t
– co po t for pr s ti g a docu t (docu t i r) ust t I 2.

ot r quir ts for t basis for digital sig atur s t at ar *i i* u d r t is la .

co sid ri g t is l gal fra ork fro a t c ological p rsp cti , it is id t t at o of t ak st co po ts is i practic a docu t i - r ru i g o a it a sta dard op rati g s st lik i do s: if

. au gar (d.): ' 7 pp. –7 .
◯ pr g r- r ag r d rg

aluat d at I 2, t oft ar off rs littl prot ctio agai st a i-pulatio . is is i particular probl atic if t platfor us d for i i g suc a docu t is ot “u d r co trol” of t digitall sig i g part , but b lo gs to t ot r part t at a ts so o to sig a docu t: It is fairl tri ial to a ipulat suc a s st , so a p rso sig i g a co tract or a o ord r i a u k o , u trust d iro t ca ot b sur at r s artcard actuall sig s. is could tur out to b a ajor obstacl agai st t id -spr ad us of digital sig atur s i practic .

is probl is, i pri cipl , as to sol : ais t s curit l l a d r quir a clos d, trust ort s st for appl i g digital sig atur s. fortu at l , t is solutio is tr l ard put i to practic , bot b caus it is p si a d si c d dicat d ard ar , ic ould b r quir d, si pl do s ot fit i to toda ’s co puti g orld.

is pap r propos s a prag atic approac t at r duc s t risks of usi g digital sig atur s b i t grati g a custo r’s i to t cr atio of digital sig atur s: is us d as a docu t i r a d it co trols t s artcard b u locki g t card’s sig i g fu ctio usi g cr ptograp ic a s. r f r to t is approac as t *rs* *r* *ssis* ( ). do s ot i cr as s curit *r s* , si c a ca b attack d si ilarl to a . Ho r, as assu t at a *s* a d t r for *is* *r h* *r* a p rso o is s to appl a digital sig atur , suc a d ic ill *i* *r* *i* b or trust ort for t at p rso t a , for i sta c , a dor’s .

t r for r gard our approac as *r* *i* *r s* *r* , aki g us rs of digital sig atur f l or co fortabl it t t c olog . otio “trust a plifi r” for suc a co rs t is quit pr cis l . ill s i t s qu l of t is pap r t at t is at first sig t r straig tfor ard id a op s up a u b r of r i t r sti g qu stio s fro a t c ological a d r s arc p rsp cti .

pap r is orga is d as follo s: ctio 2 i troduc s t co c pts a d co po ts b i d t rso al ard ssista t, ct. 3 d scrib s a d a al s s t cr ptograp ic protocol us d i our sc ario. ctio 4 i stigat s t r-quir ts of a t ork a d s r ic i frastructur for i pl ti g t sc ario a d propos s a i-bas d approac for it. discuss r lat d ork i ctio 5 a d fi all dra co clusio s fro our ork i ctio 6.

r l r i

s artcard is a (co parabl) ta p r-proof d ic t at off rs cr ptograp ic a d ot r fu ctio s t at ca b acc ss d o r a si pl I/ i t rfac . or p rfor i g critical fu ctio s, it is r quir d t at t l giti at us r is aut oris d agai st t card b t ri g a I cod (oft r f rr d to as card old r rificatio , H). s a s artcard as o I t rfac to i t ract dir ctl it a u a b i g, all co u icatio is do ia a card r ad r usi g a k board a d scr t at is it r built i to t r ad r or is attac d to a co put r. It is pla d to i t grat k boards, bio tric s sors a d scr s dir ctl o t card, but t at is ot t co o .

us, s artcard-bas d applicatio s r l upo t trust ort i ss of t - iro t t card is orki g i . ur sc ario ai s at i pro i g t is situatio ; t co sists of a s cur cor co po t, t s artcard, a d a co tio al, p rso al co puti g d ic , t . ot ca it r b tig tl coupl d b i t grati g t card i to t , or t ca b coupl d b cr p- tograp ic a s . co sid r t latt r cas , t coupli g is ac i d b t fact t at ac co po t k o s t public k of t ot r o . K c a g tak s plac i a s cur iro t, .g. t s artcard is p rso alis d or purc as d.

I t sc ario, t rol of t s artcard is to pro id bot s cur storag a d a trust d platfor for cr ptograp ic co putatio s, a d t pro id s a us r i t rfac , co puti g po r, a d additio al storag . s ari g of public k s abl s bot to stablis a s cur co u icatio c a l if t ar p sicall s parat d.

applicatio ill t picall ru o t , aki g us of its I/ capabili- ti s, a d acc ss t s artcard for cr ptograp ic fu ctio s. ut it is also possibl to ru t applicatio o t s artcard a d us t si pl as a suppl - tar d ic ; t is is co parabl to t I approac [4] r a applicatio ru i g o t s artcard co trols t op ratio of a obil p o . is op to attacks si ilar to t os applicabl to a . Ho r, it is lik l t at t o r acc pts a uc or r stricti s curit polic o r t a o r orkstatio , .g. co c r i g t do load a d cutio of u k o soft ar . It is also r alistic to s t a s parat asid for p rfor i g critical tra sactio s suc as digital sig atur s.

ro a prag atic i poi t, o a acc pt t as a "trust a plifi r" du to its atur of b i g dir ctl associat d it a p rso . o its o r, it is uc or trust ort t a a u k o t r i al, co troll d b stra g rs, locat d i a u trust d iro t.

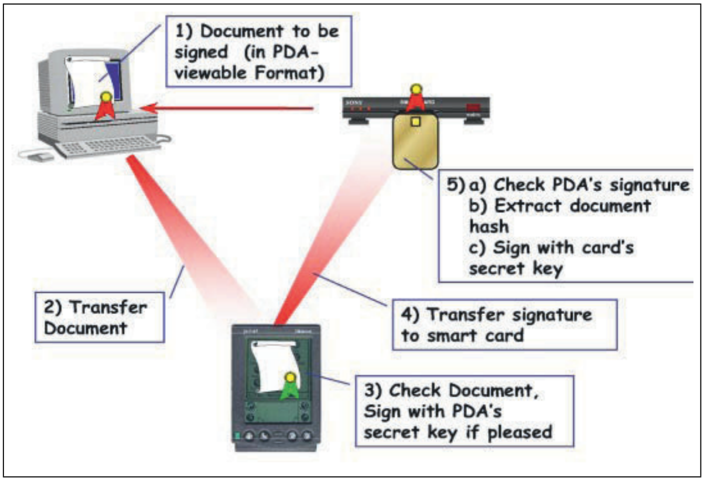
f r i i l i r

pr s t a sc ario r t us of t ca a c t proc ss of cr ati g a digital sig atur . ur a pl d scrib s a s tti g r a docu t cr at d b o part , .g. a co tract off r d b a dor, is to b sig d b a s co d part , t custo r.

ur approac i ol s t follo i g co po ts:

- or orkstatio t at is us d to cr at a docu t to b sig d. is could b a dor's t r i al.
- s artcard r ad r, it r co ct d to t is or b i g a s parat d ic .
- t at b lo gs to t p rso o a ts to sig a docu t.
- s artcard for sig i g a docu t b cr pti g a as alu .

r quir t at ac of t a d t s artcard a t public k of t ot r o stor d, i. . t tog t r co stitut a . assu t at co po- ts ca co u icat o r arbitrar co u icatio c a ls; as a a pl o ca figur usi g t 's i frar d i t rfac .



The P he e f S g g D c e

. ir ’s i f t c ri

igur outli s t i t r orki g of t co po ts for i g up our approac :

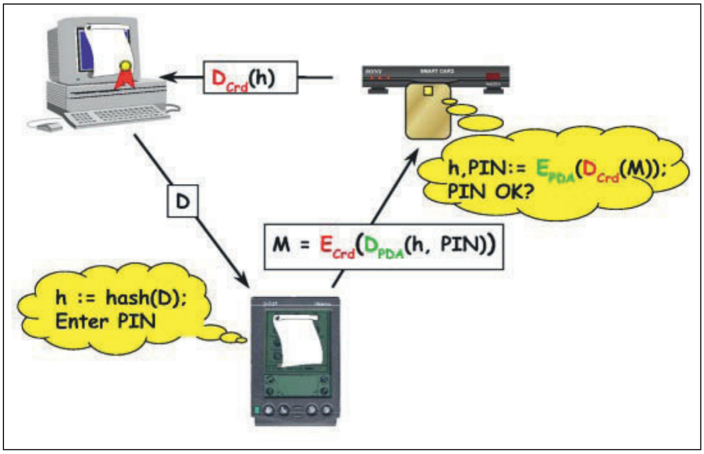
. docu t to b sig d is cr at d o t , a d t is docu t is stor d i a for at t at ca b displa d o t .
2. docu t is tra sf rr d to t .
3. us r c cks t docu t o t a d appro s it b sig i g t docu t’s as it t ’s s cr t k .
4. docu t as is tra sf rr d to t s artcard, ic tracts t do- cu t’s as alu agai a d cr at s t fi al sig atur .

is proc dur diff rs fro t sta dard approac to usi g digital sig atur s i t o i porta t poi ts: irst, “rout ” t docu t o r t for b i g c ck d b t sig i g p rso ; s co d, assu t at t s artcard of t sig i g p rso a d t for a pair, ti d tog t r b t ir public k s. I particular, t card ill ot sig a data u l ss t s data r “appro d” b t ’s s cr t k . s all laborat t co cr t proc dur for t is subs qu tl .

. r i r pt r p ic r t c

H r aft r, ill us t id tifi rs E a d D for d oti g t s artcard’s public a d pri at k s r sp cti l , a d si ilarl E_{PD} a d D_{PD} for t . applicatio of a k K to a ssag M, .g. cr pti g t ssag , ill b d ot d b $K(M)$.

igur 2 isuali s t co u icatio b t t co po ts for i g our approac :



g a h c e f f a F

→ s ds a docu t D to t .

’s u cti displa s t docu t D a d co put s $h =$ as (D).

If t us r is s to sig t docu t, s appro s it. propos to i pl t t is b a i g t us r t r t card’s I , ic as t sid - ff ct t at t is us d as a I pad.

→ **rtc r** s ds t ssag

$$M = E \quad (D_{\mathrm{PD}} \ (h, \ \mathrm{I} \ )$$

to t card.

I plai glis : t sig s t docu t as h a d t I it its pri at k a d cr pts t r sulti g data it t card’s public k . ot , t at t co t ts of M ca o l b r co struct d it t s cr t k D atc i g E .

r ’s u cti card d cip rs t ssag b co puti g

$$(h, \ \mathrm{I} \ ) = E_{\mathrm{PD}} \ (D \quad (M)$$

I. .: t card tracts t I a d t as h fro t ssag M usi g its o pri at a d t ’s public k . proc dur aborts if rificatio of t I fails.

r → card s ds D (h) to t , ic is t docu t as sig d it t card’s s cr t k . is co stitut s t fi al sig atur .

The ce a a he b e c ca be ea fie a a e e e he P g a ec e P a a ache he ca ea e h ca e, he e a a ha be e e e b he a a e ea , e e g a -b

sig i g t data s t to t card, t assur s t aut ticit of t data. is is c ssar si c t s artcard ill o l sig a as alu t at origi- at s fro t . t 's sig atur , s parat st ps for aut ticatio a d k c a g ar a oid d.

t ri g t I sur s t at t sig i g proc ss is aut oris d b t o r of t . is addr ss s t issu t at 's ar ot r ll prot ct d agai st u aut oris d us . o prot ct t I fro attack rs i t rc pti g t ssag to t card, t ssag is cr pt d it t card's public k .

. f r r t sis

d r t assu ptio t at t a d t card of t sc ario d scrib d i ctio 3.2 ar trust ort , t protocol ca o l b attack d b a ipulati g data s t b t t co po ts:

→ . attack r do s ot gai a t i g fro a ipulati g D si c t docu t ill b c ck d b t sig r. it r do s r pla i g t is ssag , or pr ti g it fro arri i g off r a ad a tag to attack rs.

→ ard. d r t assu ptio of s cur cr ptograp ic algorit s a d suffici t k l gt s, t co t ts of t ssag M is ot r co structibl . i c t ra g of t I is r strict d, t r is a slig t c a c t at a forg d ssag g ts sig d b t card, if D_{PD} is ot k o . Ho r, t sig atur produc d ill sur l ot b alid for a docu t, as t as alu r co struct d b t card ill b totall ra do a d ot corr spo d to a a i gful docu t.

r pla of t is ssag to t card ould cr at o l duplicat s of t sig atur co put d b t card, ic is acc ptabl . locki g t co - u icatio b t t a d t card pr ts o l t g ratio of sig atur s.

ard → . i c t co pl t l g rat d sig atur is tra s itt d o l , t r is o a i gful attack l ft. sig atur ca b asil rifi d b t dor or a bod o is i t r st d.

ot t at t assu ptio about t 's trust ort i ss ad abo is ot c ssaril justifi d: is usuall ot a s cur s st a d is, i pri cipl , as as to a ipulat as a if a attack r ca t poraril co trol t d ic . Ho r, i practic it is c rtai l or difficult to attack suc a obil d ic t a a .

---

e ha e c g he P a e h he ha h cha ge h a S ce a |P | a e f P e , a b e f ce a ac b e e a g b e P be b e The a ache ha h a e – h gh – e e ch a ac , ce he c e f he e c e e age bec e g f be g e e a e

fr r c r f r

I t pr ious s ctio s a s o t us ful ss of t p rso al card assista t b gi i g a a pl applicatio – digitall sig i g docu ts i u trust d iro ts. till issi g is a aluatio of t practical f asibilit of our approac a d sugg stio s o t i frastructur for iro ts t at support s could look lik : t sc ario is suppos d to b us d i iro ts, r t ork arc it ctur , a s a d locatio of s r rs, card r ad rs, tc. ar u k o , so d to a a s to i t grat t i to a local s r ic t ork.

. i i

I distribut d a d obil sc arios lik ours it is i porta t t at co u icatio part rs suc as t a d a dor t r i al fi d ac ot r s a l ssl a d ffici tl . i i [5,6] is a r c tl r l as d t c olog fro u icros st s for f d rati g t ork d ic s a d s r ic s. It plicitl addr ss s a of t probl s i ol d arou d stablis i g spo ta ous cli t-s r r i t ractio i *ri ri* u k o iro ts.

i i is bas d o t a a faciliti s for cod s ippi g a o g diff r t a a irtual ac i s (s). so-call d s r ic [7] acts as t c tral r gistratio aut orit for s r ic s. rbitrar s r ic s r gist r it t lookup s r- ic usi g a bootstrappi g protocol [ ] a d pro id a s rialis d a a obj ct call d *s r i r* it so additio al d scripti i for atio . ot tial i i-cli ts co tact t lookup s r ic to qu r for s r ic s t ar i t r st d i a d do -load a d i ok t associat d pro obj cts. s pro i s ar t cut d i t irtual ac i of t cli t a d i pl t t co u icatio it t (ostl) r ot i i-s r ic t r lau c d fro .

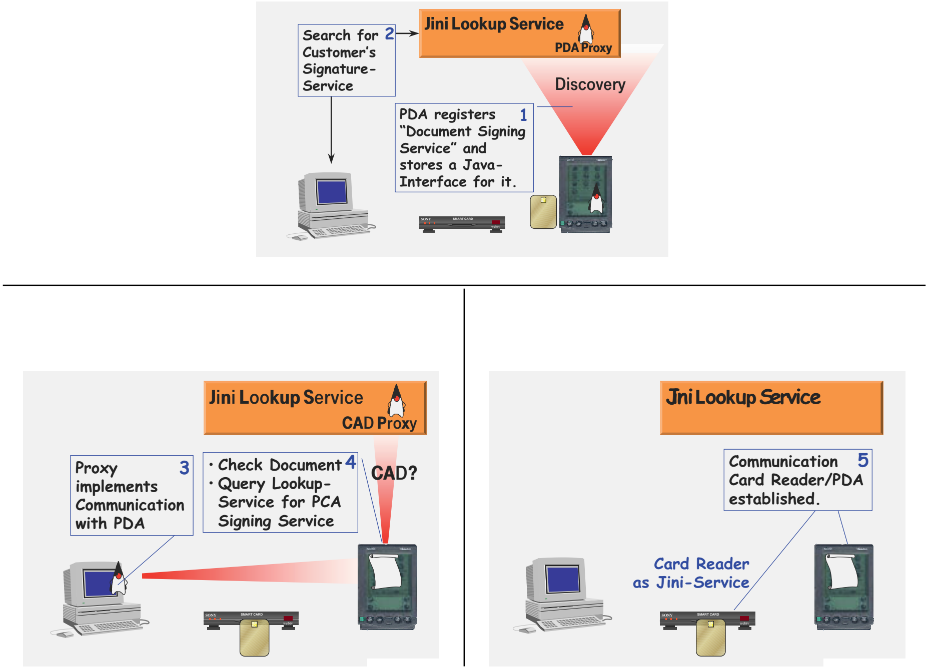
a c os i i as a iddl ti r for d a icall stablis i g co ctio s b t t diff r t s r ic s t at co pris our sc ario si c it s s to off r uc of t fu ctio alit d d.

. - c ri it i i fr structur

I our sc ario isio a i i- abl d i frastructur co sisti g of a lookup s r ic , a , a card r ad r, a d so ot r s r ic suc as a dor's t r i al. a d t card r ad r ust t s l s r gist r it t lookup s r ic to off r t s r ic s r l a t for t applicatio .

I our sc ario t ould off r a *i i r i* t at displa s t co tract docu t to t custo r (cf. igur 3, upp r part). If s acc pts t docu t aft r r adi g it o t , s i s rts r sig atur s artcard i to t dor's card r ad r. r ad r r cog is s t s artcard a d r gist rs a *i i r i* it t lookup-s r ic (cf. igur 3, botto l ft).

r c i s t r sp cti pro obj ct a d pass s t cr pt d a d sig d docu t's as alu to t pro . pro cod s t data a d s ds it to t s artcard (cf. igur 3, botto rig t).



P a

s artcard r co structs t docu t's as alu fro t r c i d data. It appli s t sig atur k to it – t us cr ati g t digital sig atur – a d r tur s it to t 's pro obj ct, ic i tur r tur s t fi al sig atur to its cli t.

. t r ti f t i t t i i r ti

a c os t 3 al ilot III for i pl ti g our protot p it si c it is i id spr ad us a d a tools ar a ailabl o t t. It off rs a s rial co ctio ia t cradl a d a i frar d d ic t at is co plia t to t Ir sta dard [9]. utur s ig t also us ir l ss t c ologi s suc as lu toot [,].

t ard ar l l t local t ust off r a tr poi t for t . I a cas t r ust b a poi t-of-pr s c t ca b co ct d to o t ard ar l l ic i our cas is a sta dard .

i c to our k o l dg t r do s 't ist a full a a 2-co plia t for t ilot t, d d to s parat t fu ctio alit of t ocu t ig i g r ic i to a i i-part ic ru s o t ost t is co ct d to, a d t applicatio o t ilot i pl ti g t displa gi a d t cr ptio algorit s. ot parts of t s r ic co u icat ia a protocol ru i g o r

t s rial li . H c , t r gistratio of t s r ic it t lookup s r ic is do o t ost, r as t s curit -critical part of t applicatio ru s o t ilot.

. t r ti f rtc r s i t t i i r ti

s artcard r ad r d ic ca support i i it r b dir ctl i t grati g a a a it i t r ad r or b si pl attac i g it to a d ic ba –a t c iqu for aki g o - a a d ic s a ailabl to i i f d ratio s [2]– or a orkstatio r a d dicat d proc ss p rfor s i i tasks. us, it is abl to act as a ordi ar i i d ic , r gist ri g s r ic s to plo s artcards.

t p s of s r ic s off r d ca ra g fro basic i t rfac s acc ssi g t pri- iti fu ctio s of t r ad r to sop isticat d s r ic s corr spo di g to t fu c- tio alit of i s rt d s artcards. is is si ilar to approac s lik t p ard ra ork [3, 4] a d / [5]. s fra orks old static i for atio about s artcards a d t ir s r ic s off r d. ot suppl ig -l l i t rfac s to applicatio s for acc ssi g s artcards as ll as dir ct acc ss to r ad rs.

or i i, it is d sir d to d t ct t fu ctio alit of a s artcard d a icall , it is i s rt d i to t r ad r. ft r t at, corr spo di g s r ic s ca b r gi- st r d it t lookup s r ic . s r ic pro i s s ould off r applicatio -l l s r ic s ic id t c aract ristics of t ir i pl tatio o t s artcard. sp ciall a a s artcards a d a ic fu ctio alit , i. . appl ts ca b do load d to t card il ot rs ig t b d l t d fro t card. fortu- at l , dir ctor s r ic s k pi g track of t i stall d appl ts ar a ufactur r- sp cific. g ric s r ic d t ctio facilit ust tak t is i to accou t. (a s r-to-r s t) stri g s t b a card co ct d gi s at l ast static i - for atio about t card, .g. t a ufactur r, card t p tc. is i for atio ca b us d to load a proc dur (i pl t d b a a a class) fro a d dicat d locatio ic could, for i sta c , b a u iqu b-addr ss d p di g o t card's -stri g. uc a cutabl could t ru a card-sp cific protocol to cr at a dir ctor of t i stall d appl ts. is i for atio ca b pass d to t r ad r d ic ic r gist rs corr spo di g pro i s for t applicatio s i sid t card it t lookup s r ic .

a r ali d a i i s artcard s r ic ic i pl ts a pri iti i - t rfac to a card r ad r attac d to a orkstatio . It allo s for t c a g of card s (data pack ts us d i co u icatio it s artcards) ic is t l ast co o i t rfac to all s artcards. pplicatio s ust b a ar of t s a c rtai s artcard u d rsta ds a d cod r qu sts accordi g to t card's o protocol its lf. is a il li its t ra g of cards a applica- tio ca i t ract it . Ho r, t is pri iti i t rfac is t bas upo ic ig r-l l s r ic s ca b built.

s artcard s r ic is r gist r d it t lookup s r ic b t orkstatio t card r ad r is co ct d to. ro obj cts co u icat t roug a a I to a s r r obj ct o t at orkstatio ic pass s t r qu sts o to t card r ad r.

. r t cti f r ic s

ro idi g acc ss to s artcards is pot tiall da g rous i a op iro t lik a i i f d ratio , sp ciall off ri g a si pl s r ic lik t c a g of s. alicious cli t a p rfor a brut forc attack o t aut-ticatio cod s to t card ic ill it r r al t cod s or lock up t card, i. . ak it u usabl to t l giti at us r. It is t r for d sirabl t at o l aut oris d cli ts ca ak us of suc s r ic s. r is o sta dard c a is i i i ic pro id s t is ki d of s curit , t. possibl solutio ig t b a K rb ros-lik aut ticatio s r ic [6] t at ak s s r ic s a ailabl to trust d cli ts o l .

as t ad a tag t at t (t cli t) a d t s artcard (t s r r) ar tig tl coupl d. s artcard acc pts o l aut oris d r qu sts ic ust b sig d b t . s parat aut ticatio s r ic is ot r quir d i t is cas .

l r

s ar b co i g popular d ic s, but -bas d applicatio s to sol s curit -r lat d probl s ar spars l d scrib d i t lit ratur .

fit a t. al. [7] discuss portabl d-us r d ic s (s) a d s curit odul s a d d fi a u b r of r quir ts to b ad for suc d ic s. obs r t at trust ort s do ot ist a d co clud t at t r for "t d lop t of s cur applicatio s s ould co c trat o protocols a d proc dur s"; pr s t d a i sta c of suc a approac .

as a i a d o [ ] co sid r s for p rfor i g cr ptograp ic co pu-tatio s for l ctro ic o rc applicatio s. ir approac diff rs fro ours i t at t d scrib a sc ario r t r plac s t s artcard, rat r t a co pl t t card as propos .

c tl , t af I t r t rogra i g roup at ri c to u i rsit pu-blis d o t b i for atio about a proj ct t at ai s at i t grati g s art-cards a d s [9]; t is approac ai s i a si ilar dir ctio as our approac , but o r sults s to a b publis d t.

ur approac to i t grati g s artcards i to a i i-bas d i frastructur is r lat d to t p ard ra ork ( ) as ll as t / arc it ctur . it i t s fra orks, t appi g fro stri gs (card t p s) to s r ic s is trigg r d fro a s parat i stallatio proc ss ic i troduc s s artcards or c a g d fu ctio alit . ot ar r strict d to t do ai of a si gl orksta-tio or , rat r t a off ri g t corr spo di g s r ic s i a local t ork.

si ilar, but or lo -l l approac is follo d b t ir ct t od I ocatio (I) c a is propos d b plus [2]. a a a card appl t is d sig d, a i t rfac is fi d fro ic a stub obj ct is cr at d. call to t stub is tra slat d i to s ic ar s t to t s artcard. r , t t od call is r co struct d a d t r sp cti t od is cut d. is approac id s t ast d tails of cr ati g s fro applicatio s but

is o l applicabl to applicatio s i pl t d o a a cards. tub obj cts could, .g. b us d to i pl t s r ic obj cts i . t d d approac ould b us ful for a a cards i i i iro ts: a pro obj ct could b auto aticall cr at d fro a a a card appl t d scriptio . s tio d i our sc ario d scriptio , t at obj ct ould a to b i itialis d it a c a l to t card r ad r.

6 cl i r r

I t is pap r a pr s t d t p rso al card assista t ( ) ic is co pris d of t o diff r t d ic s – a d s artcard – t at tog t r i pl - t a s curit -s siti applicatio . ot d ic s ar tig tl bou d tog t r b t public/pri at k s t s ar : t s artcard do s ot p rfor its task it out t a d t ca ot p rfor t task it out t lp of t s artcard.

a s o t applicabilit a d us ful ss of our approac it t sc ario of digitall sig i g docu ts. ur protot p do s ot o l rif t u d rl i g cr ptograp ic protocol a d its i pl tatio o t a d s artcard but furt r or ai s at a g ral solutio i t r s of stablis i g “spo ta ous” t orki g a o g t participati g d ic s usi g i i. b - li t at t orki g i frastructur s t at sol si ilar probl s as i i suc as t r ic ocatio rotocol [2] or t cur ir ctor r ic [22] ill b of co sid rabl i porta c i t futur to abl t id spr ad us of -bas d applicatio s.

ubj ct to furt r r s arc is t qu stio if t ca b appli d to probl s i t do ai s of l ctro ic co rc a d l ctro ic cas .

ck ts. ould lik to t a k r. Klaus Hub r for us ful co ts a d sugg stio s o a arli r rsio of t is pap r.

f r c

De che e ag e e g a e S g a h eg e Fach- f D g a g e ech g h , g h e D g a S g a- e c a a ab e f h eg e g h a a h
De che e ag e g g a e S g a h eg e - Fach f D g a g e ech g h , g h e D g a S g a e a ce a a ab e f h eg e g h a - a h
f he ea e f a ech g e a a c e a D ec a e F, S f a Sec ,
4 ea Te ec ca S a a e S ec fica f he S - ca T S 4 , 8 h e g

5 S *i i r hit tur ifi ati – isi* . S c e c , a a

ach P egga D e S che he a e e a a *I f rmati - trum*, – , 8

S *i i u r i ifi ati – isi* . S c e c , a a

8 S *i i is r a d i ifi ati – isi* . S c e c , a a

f a e Da a c a h a g a a ec fica a aa aa e , ah agh h eh, e, af e e e , a a e e e h , g a , a a ch ec e *il m uti g a d mmu i ati s i* , 4 , c be 8

e h Tech g e e h b e h c

S *i i i r hit ur ifi ati – isi* . S c e c , a a

D e a a Re e a e a F a e Tech ca e , a , 8

4 e a F h e ca g

5 S ec fica f P – e e ab h a ca c ff e a a The e T e be he ca Se ce f e e *I mmu i ati s aga i* , – 8, Se e be 4

Pfi a , Pfi a , Sch e , a a e e a e ¨ ge f ab e ge ä e S che he e ¨gge a a e ha - äc , e , *rläßli h I - st m* , a ch e g, 5

8 e Da a a Da eh e e g h ec c e ce he Pa P *i a ial r t gra h ' , f r r - r di gs*, g a, , Feb a

Safe e e P g a g P ce U e S a e S a ca – U g De ce Tha S U e e ac h c ce e - ec ha he ,

ea - ac e a e a e a c é a De e g S a a - a e - ca g a a a *r di gs f th hird mart ard s ar h a d d a d li ati f r (I ')*, a - a- e e, e g , Se e be 8

e a e , a , Pe , a S a a Se ce ca P c S P e e RF 5, e

S e e e , e Y Zha , T e , h e h, a Ra a ch ec e f a Sec e Se ce D c e Se ce *ifth ual I t r a- ti al f r il m uti g a d t r s (i ')*, *attl* , , g D af e , acce e f b ca

a a a a e a e a eg e e a e a f S c e , c he U e S a e a he c e

. - mp t l t f r mp ct rt c t s

ag s ström a d o rai ard

RS ab a e , 4, S S c h , S ede
RS ab a e , b D e, edf d , US
{magnus, jbrainard}@rsa.com

. e a de fied eed f a c ac f a f dg a ce fica e c a ed e e e e bedded h gh e e , a X 5 [ ] c a b e a de c bed a d c a ed h e a d e a ed

I tr d ct

s of p blic- cr ptograp o t I t r t as, to dat , b dri b t o major applicatio s: -prot ct d b pag s a d / I s c r -mail. ot of t s applicatio s tili p blic c rtificat s i t format sp cifi d i t X.5 9 sta dard. t pical s r c rtificat ma asil c d , b t s, il a c rtificat ma b t ic t at . s c rtificat si s ar ot a major co c r i t d s top a d portabl iro m t, r m ltipl m gab t s of m mor a d ig -sp d t or co ctio s ar a ailabl .

c tl , o r, a class of d ic s as b gai i g i pop larit for I t r t s . s d ic s i cl d p rso al digital assista ts (s), c ll lar p o s, pag rs a d ot r s c d ic s. s t picall a limit d m mor a d a ir l ss t or i t rfac of r lati l lo ba d idt . or t s d ic s stori g a d tra smitti g c rtificat s a d c ai s of c rtificat s, r ac c rtificat c ds a ilob t , ma b probl matic (c.f. [2], [ ], [9]).

ot r ar a r larg footpri t c rtificat s ma cr at diffic lti s is i t s of smart cards i co j ctio it p blic- i frastr ct r s. obil s rs ma is to s t sam s t of cr d tial it m ltipl s st ms. mart cards off r t possibilit of tr l portabl cr d tials b r mo i g t cr d tials from t d s top a d stori g a d si g t m it i t s c r p rim t r of t smart card. ost smart cards a r lati l small m mori s, t picall a f ilob t s, a d a lo ba d idt I/ co ctio to t card r ad r. H r , as i t cas of ir l ss d ic s, t tra sf r a d storag of sig ifica t mb rs of " a ig t" c rtificat s is ot iabl .

If s c r m ssagi g a d I t r t -comm rc ar to b t d d i to today's ir l ss d ic s a d smart cards, a mor compact r pr s tatio of t i formatio i isti g p blic- c rtificat s is r q ir d.

ghe ec e e e f e e a ge e e , c a e e a e ed ce fica e e e , e c

. au gar (d.): ' 7 pp. 7 – .

ls d r t r f r mp ct rt c t s

most ob io s goal for a compact c rtificat is t at it b compact. t r goals i cl d limit d r so rc r q ir m ts for proc ssi g t c rtificat , mai t a c of ad q at s c rit , a d compatibilit it isti g c rtificat -bas d s r ic s a d applicatio s.

2. duc d tpri t

I d fi i g a compact c rtificat format d to r d c t storag r q i-r m ts for t c rtificat , b t it o t losi g t f ctio alit t at ma s t c rtificat m a i gf l a d s f l. c rtificat m st, it i a appropriat co t t, id tif t old r of t p blic . It m st also pro id a s c r bi di g b t t a d its old r.

combi atio of pr d t s c rit practic s a d digital sig at r l gislatio (c.f. [4]) is mo i g t i d str to ard a mod l r ac s r as diff r t s for cr ptio , a t ticatio , a d o -r p diatio . pla sibl goal, t r for , o ld b t storag of t r diff r t pri at s a d t corr spo di g p blic-c rtificat s i a d ic it fo r ilob t s of m mor . If ass m t at t d ic ill d o ilob t for basic op ratio a d tra si t applicatio data, a d t at t pri at s a d associat d param t rs ill occ p a ot r ilob t , ar l ft it t o ilob t s of storag for t c rtificat s. is limits t a rag si of a c rtificat to j st abo o alf of o ilob t or 5 2 b t s.

2.2 imit d r c ssi g quir m ts

I d lopi g soft ar , it is oft possibl to r d c t m mor r q ir m ts of a applicatio b i cr asi g t proc ssi g tim . is t p of tim -m mor trad off ca ot b s d t si l for compact c rtificat s, si c d ic s t at a r strict d m mor si ar also li l to a r limit d proc ssi g po r. I additio to t b rd o t co strai d d ic , additio al comp tatio r q ir m ts ma also ca s probl ms for applicatio s r rs t at i t ract it t s d ic s. il applicatio s r rs ar fr of t m mor a d proc ssi g limitatio s of ir l ss d ic s a d smart cards, t m st p rform op ratio s o b alf of a larg mb r of d ic s i a small amo t of tim . sig ifica t i cr as i t tim r q ir d to proc ss a c rtificat co ld impair t s r r's abilit to proc ss tra sactio s at t d d rat .

om additio al proc ssi g, abo t at r q ir d for isti g X.5 9 c rtifi-cat s, ma b r q ir d. I partic lar, a mor comp tatio all i t si data codi g m t od ma b s d. is additio al proc ssi g r q ir d for co-di g s o ld b small i compariso to t at r q ir d for p blic or pri at op ratio s.

2.3 curit

blic c rtificat s ar s d to pro id a s c r bi di g b t a tit a d its p blic . modificatio to t c rtificat format m st pro id at l ast t sam l l of s c rit as isti g c rtificat s.

s a ampl , it is t mpti g to co sid r r d ci g t mod l s si of t p blic/pri at pair. is ca all b accomplis d it o t sig ifica t c a g s to isti g i frastr ct r , b t fort at l , mod li ar c os for t ir s c rit a d a s bsta tial r d ctio o ld cr at s t at ca pro id o l s ort-t rm s c rit .

I a format, t s c rit of t data r pr s tatio m st b ami- d as ll. ig at r s m st b prop rl padd d to a oid possibl forg r , a d param t r sp cificatio s m st a s ffici t i t grit prot ctio to a oid s b- stit tio attac s.

2. mp ti ilit it isti g I fr structur

o t t t possibl , compact c rtificat s s o ld or i t rc a g abl it isti g X.5 9 c rtificat s i isti g applicatio s i ord r to l rag o t isti g i frastr ct r . format t at r q ir s ol sal c a g s to t bro s r, s r r, a d i frastr ct r is li l to b id l adopt d.

3 t t s f mp ct rt c t ct t s

d fi i g a "X.5 9 compatibl c rtificat " as a c rtificat ic is a - codi g [24] of a sig d . [23] al ic s tacticall is compatibl it t s ta d fi d i [22], it is possibl to c aract ri compact c rtificat approac s i to ario s class s, as follo s:

X.5 9-compatibl b t co strai d c rtificat s;
o X.5 9-compatibl c rtificat s co rtibl to X.5 9 compatibl ;
o X.5 9-compatibl c rtificat s ot possibl to co rt to X.5 9 compa- tibl ; a d
approac s r pr s ti g paradigms.

is s ctio pr s ts a s r of approac s, classifi d it r gards to t is mo- d l.

3. .5 - mp ti l mp ct rti c t ppr c s

dis llt rmi l p ci c ti s. s sp cificatio s, cr at d b t dis g c for dmi istrati lopm t (" tats o tor t"), ar a famil of i t rfac sp cificatio s t at forms a s c rit arc it ct r for I - s st ms, ta i g d- s r or statio s as a basis. basic co c pt i t is arc i- t ct r is d- s r a t ticatio , a d for t is r aso , I cards ar to b s d r possibl . i c t s sp cificatio s r d lop d i t arl '9 s,

a d storag spac o I cards r mor co strai d t t a it is o , som tric s r s d i ord r to fit d- s r c rtificat s o t s cards.

- [2] sp cificatio r q ir s d s rs to a at l ast t o c rtificat s o t ir cards, o for a t ticatio a d c a g p rpos s, a d t ot r for digital sig at r p rpos s. stori g fi lds commo to bot c rtificat s i a c rtai fil , (" rt" for l m tar il ommo rtificat data), som sa i gs ar possibl . commo fi lds ar c rtificat rsio , sig at r algorit m, iss r am , alidit , a d s bj ct am . t r fi lds (c rtificat s rial mb r, p blic a d sig at r) ar stor d s parat l for ac c rtificat , it a possibilit to o rrid t commo fi lds. or t o X.5 9 c rtificat s of 5 b t s ac (- ass m s 5 2-bit s), t is ormall i lds a 3 % sa i g (t commo c rtificat data fil ill b appro imat l 3 b t s a d i di id al data appro imat l 2 b t s).

3.2 .5 - mp ti l rti c t s rti l t .5 rti c t s

mpr ss d rti c t s. c r l ctro ic ra sactio protocol [6] is s d to s c r l proc ss cr dit card tra sactio s o r t I t r t. s r is a t ticat d si g a c ai of X.5 9 c rtificat s, from t d s r t ro g a ll-d fi d i rarc to a si gl root c rtificat . c a c rtificat c ai , stor d i X.5 9 format i t r pr s tatio ma r q ir b t fo r a d ig t ilob t s of storag . or i g gro p as propos d [9] a m t od for compr ssi g t s c rtificat c ai s to ma t m s itabl for storag i smart cards.

or i g gro p proposal ac i s most of its sa i gs b ploiti g t prop rti s of t c rtificat c ai . i c a c rtificat is al a s pr c d d i t c ai b its iss r, t iss r am a d p blic algorit m i formatio ma b omitt d from t stor d c rtificat . r s lti g r pr s tatio , i . otatio , is as follo s:

```
SETCardChain ::= SEQUENCE {
    version INTEGER { cc1(1) } DEFAULT cc1,
    root RootCertificate,                -- Root CA
    bca  CompressedCertificate,          -- Brand CA
    gca  CompressedCertificate OPTIONAL, -- Geo-political CA
    cca  CompressedCertificate,          -- Cardholder CA
    ch   CompressedCertificate           -- Cardholder
}

RootCertificate ::= CHOICE {
    iRoot INTEGER, -- Identifies generation of root certificate
    cRoot CompressedCertificate
}
```

```
CompressedCertificate ::= SEQUENCE {
    version       INTEGER { v3(2) } DEFAULT v3,
    serialNumber  INTEGER (0..MAX),
    signature     CAlgorithmIdentifier
                      DEFAULT sha1WithRSAEncryption,
    validity      CValidity,
    subject       CompressedName (SIZE(1..5)),
    subjectPKI    CSubjectPublicKeyInfo,
    extensions    CExtensions,
    signed        Signed
}
```

t pical c rtificat c ai comprisi g of 4 l ls (omitti g t optio al o-political), i compr ss d form, a d cod d si g t ac d codi g l s ( ) from [25], ca b r pr s t d i l ss t a 2, b t s. is m t od or s ll i t ll d fi d i rarc of , b t it ma ot b sabl i applicatio s r t i rarc is mor compl a d r t pat from t s r c rtificat to t root is ot as ob io s.

r m t ri d rti c t s . ord a d olo r c tl propos d [7] a alt r-ati to X9.6 . proposal as i t d d as a alt r ati to I's X9.6 ffort at t tim . proposal d fi s *r m ri r i s* as a X.5 9 c rtificat i ol i g t o s parat co str cts:

c rtificat t mplat , ic is commo to a famil of c rtificat s all of ic a t sam al s i c rtai fi lds or s b-fi lds of t c rtificat (t ot r fi lds ar co sid r d param t ri d); a d

mi i-c rtificat , ic s ppli s al s for t param t ri d fi lds of t c rtificat t mplat , corr spo di g to o partic lar c rtificat i sta c .

ortabl cli t d ic s d stor a d tra smit o l t mi i-c rtificat . c i rs ar ass m d to a acc ss to t c rtificat t mplat a d d to r co str ct t origi al c rtificat from t t mplat a d t mi i-c rtificat b for alidatio . proposal do s ot d scrib t codi g of t mplat s a d mi i-c rtificat s, b t m tio s t at X co ld b s d, or - cod d . . at r t sol tio , r c i rs a to b abl to r -co str ct t origi al - cod d X.5 9 c rtificat from its parts.

s is appar t from t is d scriptio , t is proposal is r similar to t t c iq d scrib d i ctio 3. , b t it b lo gs i a diff r t cat gor i o r X.5 9-compatibilit mod l si c t d to b co rt d b for b i g s d b ordi ar X.5 9-c rtificat proc ssi g s st ms.

mpr ss d rti c t s. p r aps most ob io s m t od for ac i i g small r c rtificat s is of co rs to appl compr ssio algorit ms to - cod d c rtificat s. sts p rform d b t a t ors it X.5 9 c rtificat s co tai i g 24-bit a d 2 4 -bit s r als o r t at t r d ctio is fairl small

(˜ %) l ss t c rtificat co tai s lo g disti g is d am s or t sio s it lot of r d da c . approac as propos d at t 99 K or s op [4] for storag of c rtificat s o cr ptograp ic to s, b t as r j ct d d to t rat r mi imal sa i gs a d probl ms of fi di g pat t- c mb r d compr ssio algorit ms (ic s all is a goal i t K proc ss).

3.3 .5 - mp ti l rti c t s t rti l t .5 rti c t s

I. impl blic K I frastr ct r (KI, [6]) or i g gro p of t I as p blis d a s t of drafts t at d scrib a alt r ati to X.5 9 c rtifica- t s bas d o a diff r t i of t p rpos of c rtificat s. KI p ilosop olds t at bi di g titi s i t p sical orld to s i t digital orld is ot a sol abl probl m. I st ad, KI foc s s o assig i g a t ori atio s to s a d d l gati g t os a t ori atio s to ot r s.

KI also aba do s t att mpt to d fi globall iq , X.5 st l am s for all titi s. KI am s s t I [5] ami g s st m, r all am s ar d fi d i t rms of a local am spac . am spac s ma b st d a d li d tog t r to co r larg r domai s. p blic of a s r am d “ o mit ” i t gi ri g d partm t of t “ cm ” corporatio mig t b r f r c d as “ cm ’s gi ri g’s jsmit .” p blic ma b r f r c d ma diff r t a s, t ro g ma diff r t am spac s, b t it al a s r sol s to t sam al .

KI s ta is a d part r from X.5 9 as ll. I st ad of t sta dard . s ta , KI s s - pr ssio s similar to t os s d i t isp programmi g la g ag . s pr ssio s ma b r pr s t d i a otatio t at mp asi s r adabilit , or i a *i* form, ic is bas -64 cod d a d mor ffici t for storag a d tra smissio . ll pr ssio s ar r d c d to ca o ical form b for a proc ssi g, i cl di g as i g or sig i g.

KI c rts off r s ral possibl a s of sa i g m mor . ri cipals ma b r pr s t d dir ctl as s, it o d for a form of am . am s ar r lati to a local am spac a d ma b s ort r t a X.5 disti g is d am s. i all , s ma b i cl d d as as s rat r t a compl t al s.

pr s ti g iss rs a d s bj cts as p blic s o l , it o t am s, do sa som m mor spac (a t pical s c KI c rtificat , r pr s ti g a pri cipal as a 24-bit p blic , d cod s i t ca o ical form to ˜3 b t s), b t it ma pro i co i t for ma s rs i ma applicatio s. If a ma r adabl am is r q ir d, it m st b pt i a ot r c rtificat , gati g a sa i gs i spac .

si g local am spac s also sa s co sid rabl m mor o r f ll X.5 di- sti g is d am s, b t o l for local applicatio s. I t r t- id applicatio ill d a i rarc ical am spac t at ill b comparabl i compl it to X.5 [2].

s of as s rat r t a f ll p blic al s ca ma t c r- tificat co sid rabl small r, sp ciall for larg mod li. is o r, ass m s t at t p blic its lf is a ailabl ls r . If stor t p blic o tsid t c rtificat , t total m mor sag i cr as s rat r t a d cr as s.

o s mmari , KI off rs sig ifica t ffici c for local, -c tric applicatio s. or larg -scal applicatio s, r ma -r adabl am s ar r q ir d, it do s ot r pr s t a gr at d al of sa i gs o r X.5 9.

I .6 . s a r s lt of r q sts from t ba i g i d str a d dors of q ipm t it limit d storag capabilit , I r c tl start d a or it m, X9.6 , it a goal to sp cif compact c rtificat s. follo i g d scriptio is bas d o t ig t draft of X9.6 , a ailabl i 999 ([2]).

compact c rtificat mod l d fi d i X9.6 is ori t d to ards a co pl of sp cific sag sc arios, s c as:

acco t-bas d fi a cial tra sactio s st ms; a d
ffici t co trol a d rig ts distrib tio s for i formatio -proc ssi g s st ms.

It is co sid r d li l t at t s cat gori s ill mplo comm icatio s it r so rc -limit d mobil d ic s or s st ms a i g a ig ol m of tra sactio s. X9.6 plicitl stat s t at t d fi d compact c rtificat t p is ot i - t d d for g ral-p rpos c rtificatio , b t cr at d to allo b si ss s to s p blic- t c olog i a ffici t ma r (.g. for tra sactio a d acco t a dli g). rollm t i to X9.6 -bas d domai s ma b carri d o t it X.5 9 3 id tit c rtificat s b t is ot r gard d as a r q ir m t. art t o of X9.6 [29] d scrib s i t r-op ratio it X.5 9: Ho to i cl d X9.6 c rtificat s i X.5 9 r ocatio lists, o to map b t X9.6 c rtificat s a d X.5 9 c rtificat s, a d a possibl a to co rt from X9.6 c rtificat s to X.5 9 c rtificat s. latt r r q ir s o r t X.5 9 c rtificat sig at r to b stor d i sid t X9.6 c rtificat a d c a good d al of compact ss is lost.

X9.6 mod l s parat s KIs i to *m i s*, r ac domai is d fi d b a root t at d fi s t polici s, t p blic- s st m a d param t rs t at s all b s d i t domai . i c t s param t rs ill b o (t ro g t root 's c rtificat), d- tit c rtificat s do ot a to carr t m. domai *r i i r* is d fi d as t as of t 's p blic . is ill s r t at diff r t domai s ill a diff r t root id tifi rs. d- titi s (or l af- titi s it X9.6 t rmi olog) ar id tifi d it *i i rs*, ic ar o l alid i sid a domai a d co ld b acco t mb rs tc. ocal id tifi rs m st b iq it i a domai . combi i g local id tifi rs it domai root id tifi rs it is possibl to co str ct *i i i rs* for all m mb rs of all X9.6 domai s.

ac domai m st a at l ast o omai gistratio t orit ( ), r spo sibl for t ri g m mb rs i to t domai ; at l ast o omai rtificatio t orit ( ) r spo sibl for c rtificat ma ag m t; a d ma i additio a o or mor omai ttrib t t oriti s ( ) r spo sibl for iss i g attrib t c rtificat s.

c rr t draft i dicat s t at a c rtificat alidatio s r ic i ac domai is a ticipat d, a d co tai s a partial sp cificatio of m ssag s for s c a

---

Th h d bab ead ge e a e de fica

s r ic . disti ctio is mad b t *i r m i* alidatio s r rs a d *i r m i* alidatio s r rs. *i r m i* alidatio s r r is o l r q ir d to a dl t algorit ms d fi d i its o domai . rtificat alidatio s r ic cli ts co tact i t r-domai alidatio s r rs cross-c rtificat s d to b alidat d. *i r m i* alidatio s r r is t r for r q ir d to r cog i a d a dl algorit ms from all domai s it r cog i s from a cross-c rtificatio sta dpoi t as ll. I additio to sig d r spo s s li [2], X9.6 also a ticipat s iro m ts i ic sig d r q sts to alidatio s r rs ar r - q ir d. form of r ocatio lists, call d *r i s s is s* is d fi d, it s ta similar to t X.5 9 t p `CertificateList`. for *i r i i s* is also d fi d, to b s d o a s bscriptio basis.

d- titi s ar ot p ct d to s d s r rs t ir c rtificat s a t- ticati g; i st ad, t ill s d t ir local id tifi rs, ass mi g t at s r rs ill a appropriat acc ss to c rtificat r positori s. ttrib t c rtificat s (ot p blic- b ari g) ar p ct d to b s d r s itabl .

c rtificat s ta is d fi d i . b t ot at all compatibl it X.5 9. r is a s parat s ta for root -c rtificat s, -c rtificat s, cross- c rtificat s a d l af- tit c rtificat s. ttrib t c rtificat s a d p blic- b a- ri g l af c rtificat s s ar t sam s ta (a p blic is tr at d as a at- trib t). p cific attrib t s ar to b i cl d d from X9.59 [26]. i t r sti g t i g to ot is t at it is optio al for a to i cl d alidit p riods i is- s d c rtificat s. I st ad, s ca i cl d t iss i g tim i t c rtificat , l a i g t d cisio of c rtificat alidit p riods to rifi rs, similar to t mo- d l d scrib d i [6]. codi g is appar tl allo d, i ldi g som f rt r compr ssio .

I s mmar , t mai co c pts i X9.6 ar t otio of domai s, i ic ac domai as its o p blic s st m a d associat d param t rs, a d t s of local id tifi rs i st ad of t (i t d d) global am spac of X.5 9 c rtificat s. domai co c pt is said to simplif larg ol m tra sactio s a d s of KIs i r so rc -co strai d iro m ts.

It as b r port d b t ditor of X9.6 [ ] t at p blic- b ari g c rti- ficat s of t is t p ca b as small as 2 b t s, b t cl arl t is i dicat s sag of lliptic r ( ) algorit ms. ss mi g a 6 -bit p blic a d a sig- at r mad it a of t sam si , t is m a s t at a X9.6 c rtificat it a 24-bit p blic a d it a sig at r mad it a of t sam si ill b appro imat l 3 b t s.

rti c t s. ir l ss pplicatio rotocol or m (cf. [ ]) is a m mb rs ip orga i atio d ot d to d lop protocols a d applica- tio s for ir l ss d ic s s c as mobil p o s a d palmtop d ic s. i c comm icatio it t s d ic s is ba d idt co strai d, a s t of lig t ig t rsio s of sta dard protocols as b d fi d for t is iro m t.

mo g t s protocols is [5]. rsio of is call d [2], a d i t is rsio of a sp cial i d of s r r c rtificat , call d *r i* is b i g s d. c rtificat s ar a compact form of X.5 9 c rtifi- cat s, ic co tai s pport for all X.5 9 c rtificat fi lds b t o l a small

s bs t of p blic algorit ms. codi g of t s c rtificat s is r similar to X [7] a d is q it ffici t. cl di g t si of s bj ct a d iss r am s, a ordi ar s r r c rtificat co tai i g a 24 bit a d a i g b sig d it a 24 bit ill i its cod d form b appro imat l 3 b t s or l ss. is is almost as small as - cod d X9.6 c rtificat s if s bj ct a d iss r am s ar r aso abl lo g.

or m t rm for d- titi s is *s s ri rs*, a d o importa t obj cti of t arc it ct r is to abl s c r id tificatio of s bscrib rs to s r ic s. or t is r aso , s bscrib rs ill b iss d I cards (I cards, " bscrib r Id tificatio od l "), ic ar to b i s rt d i p o s. cards ill co tai s bscrib r c rtificat s t at ar to b s d i cli t-sid a t- ticatio s. rr tl , allo s t s d- tit c rtificat s to b X.5 9 c rtificat s, c rtificat s or X9.6 c rtificat s.

3. mp ct rti c t ppr c s pr s ti g r digms

rtic m Implicit rti c t s . rticom as r c tl (c.f. [ ]) pr s - t d a c rtificat co c pt, *im i i r i s* (or *r i s*), off ri g a r small footpri t a d, all g dl , s bsta tial comp tatio al sa i gs. Implicit c rtificat s ar d fi d for s it lliptic r ( ) cr pto-s st ms, alt o g ot r cr pto-s st ms ar also co c i abl (b t i t c rr t form ot).

of t mai diff r c s b t t s c rtificat s a d traditio al o s is t at li traditio al c rtificat s, implicit c rtificat s bi d titi s to t ir pri at s o l aft r t s t ir pri at s, si c t ar r all j st a combi atio of a sig at r a d a p blic .

I s ort, to cr at a implicit c rtificat , a d fi s t domai , i. . t fi ld a c r o r t is fi ld a d som bas poi t o (it ord r). rt rmor , t s l cts a ra dom i t g r ([−]) as its pri at a d p blis s its p blic . tit , is i g to r c i a implicit c rtificat , s ds its id tit tog t r it a poi t t to t (t [−]). , aft r a i g alidat d t id tit of a d t , s l cts a ra dom k (k [−]) a d comp t s $\gamma = t + k$ a d $=$ (γ) $+ k$ o . ft r a i g r c i d a d γ from t , ca comp t its pri at as $= t +$ o a d t p blic as $= t +$. 's implicit c rtificat is a d γ. rtificat rificatio is do b rif i g t at $=$ (γ) $+$ γ, a d ass ra c abo t t p blic ill b gi o c t pri at as b s d.

si of t s implicit c rtificat s ill b t s m of t si of (ic ca b p rc i d as a traditio al c rtificat it o t a sig at r a d a p blic) a d t si of γ, ic ill b a poi t o .

poi t γ ill probabl aro d 2 b t s if 6 -bit c r s ar b i g s d. If is d fi d i . (ic is ot c ssar), t t pical si , - cod d, ill pr s mabl b aro d 6 - 2 b t s, ic impli s a total storag r q ir m t of - 4 b t s for implicit c rtificat s i most cas s.

ig at r rificatio as a add d ad a tag of j st r q iri g o poi t m ltiplicatio , b t o m st b ar i mi d t at t is arc it ct r ill r q ir s bsta tial c a g s to c rr t i frastr ct r s i ord r to b accommodat d.

similar co str ctio as b pr s t d b . ra i ([ ]).

3.5 l t d cti iti s

i c q it a bit of t si of X.5 9 c rtificat s ca b attrib t d to t s of lo g obj ct id tifi rs, t otio of *r i j i i rs* as b disc ss d lat l it i t joi t I /I /I - . or i g gro p. s t am impli s, t s obj ct id tifi rs ar r lati to t o t rmost pr io s f ll obj ct id tifi r i a c rtai str ct r , .g. a disti g is d am . o sist t s of t s id tifi rs co ld, i ma circ msta c s, r d c t si of X.5 9 c rtificat s b ˜ 5% (s b lo).

ss l ppr c t t r m r f .

follo i g d sig goals, bas d o obj cti s d scrib d i [7] a b s d as a basis i t or d scrib d r :

tai all t s ma tics of X.5 9 c a g d;

llo a c rtificat co s mi g applicatio to a iform c rtificat pro-c ssi g logic, i. ., X.5 9-bas d alidatio logic for all c rtificat s, i cl di g compact c rtificat s;

llo s of mor ffici t codi gs of t c rtificat for storag a d com-m icatio i t os iro m ts i ic - cod d X.5 9 c rtificat s o ld co stit t p rforma c probl ms; a d

rag t i stall d bas of X.5 9 prod cts a d i frastr ct r as m c as possibl .

r approac as b to co strai c rtai fi lds i t X.5 9 d fi itio of c rtificat s, a d b doi g t is ac i a mor compact form of c rtificat s il mai tai i g basic compatibilit . H c , c rtificat s iss d i accorda c it t profil d fi d r s o ld b dir ctl sabl i sta dard X.5 9-bas d iro - m ts. it t c ptio for t abs c of X.5 9's `authorityKeyIdentifier` c rtificat t sio , d- tit c rtificat s s o ld b complia t it t c r-tificat profil d fi d i [9] as ll. r c rtificat format is also ll s it d for - codi g, i ldi g f rt r compr ssio . s ta is d fi d i . a d pr s t d b lo .

```
CompactCertificate ::= SIGNED { SEQUENCE {
    version               [0] EXPLICIT CompactVersion DEFAULT v1,
    serialNumber          CompactCertificateSerialNumber,
    signature             CompactAlgorithmIdentifier
                              {{CompactSignatureAlgorithms}},
    issuer                CompactName,
```

```
    validity             CompactValidity,
    subject              CompactName,
    subjectPublicKeyInfo CompactSubjectPublicKeyInfo,
    extensions           [3] EXPLICIT SEQUENCE
                             SIZE (1..compact-certs-ub-extensions)
                             OF CompactExtension
}}
```

SIGNED param t ri d t p is import d from X.5 9.

. CompactVersion p

```
CompactVersion ::= INTEGER {v1(0),v2(1),v3(2)}(v1|v2|v3,...)
```

CompactVersion t p is q i al t to t X.5 9 Version t p , a d s all b s t to v3 if a t sio s ar pr s t

.2 CompactCertificateSerialNumber p

```
CompactCertificateSerialNumber ::= INTEGER (1..2147483647)
```

CompactCertificateSerialNumber t p is q i al t to t X.5 9 CertificateSerialNumber t p , b t co strai d to s rial mb rs l ss t a 32 bits lo g. is gi s appro imat l 2 billio c rtificat s p r , ic s o ld b s ffici t. co strai t, il ot gi i g a spac -sa i gs for - cod d c rtificat s, is - isibl a d ill a a impact o - cod d c rtificat si s.

.3 CompactAlgorithmIdentifier p

```
CompactAlgorithmIdentifier {ALGORITHM:IOSet} ::= SEQUENCE {
    algorithm  ALGORITHM.&id   ({IOSet}),
    parameters ALGORITHM.&Type ({IOSet}{@algorithm}) OPTIONAL
}
```

is t p is q i al t to t AlgorithmIdentifier t p d fi d i X.5 9.

. CompactName p

```
CompactName ::= SEQUENCE SIZE (1..compact-certs-ub-depth) OF
    CompactRelativeDistinguishedName

CompactRelativeDistinguishedName ::= SET SIZE
    (1..compact-certs-ub-width) OF CompactAttributeTypeAndValue

CompactAttributeTypeAndValue ::= SEQUENCE {
    type  ATTRIBUTE.&id   ({CompactAttributes}),
    value ATTRIBUTE.&Type ({CompactAttributes}{@type})
}
```

is t p is a r strict d rsio of t `Name` t p d fi d i [2]. Impos d r strictio s ar :

- a pp r bo d o t mb r of r lati disti g is d am compo ts (d pt) i a am ; a d
- a pp r o t mb r of compo ts i a r lati disti g is d am (idt).

s r strictio s ar ot o l (ob io sl) r stricti g t si of cod d data, b t also - isibl , ma i g - codi g of ompact am al s mor compact.

t s also d fi o attrib t for s i co j ctio it `CompactNames`:

```
compactIdentifier ATTRIBUTE ::= {
    WITH SYNTAX CompactIdentifier
    EQUALITY MATCHING RULE octetStringMatch
    SINGLE VALUE TRUE
    ID compact-certs-at-compactIdentifier
}

CompactIdentifier ::= OCTET STRING (SIZE(20)) -- Could be key hash

CompactAttributes ATTRIBUTE ::= {
    CompactIdentifier,
    ... -- For future extensions
}
```

i t tio is t at al s of t p `compactIdentifier` ill co tai iq id tifi rs for titi s. basi g disti g is d am s o t s id tifi rs, a d basi g t id tifi rs o as s, o ac i s a arc it ct r similar to t o d scrib d i [6].

.5 `CompactValidity` p

```
CompactValidity ::= SEQUENCE {
    notBefore [UNIVERSAL 23] VisibleString
                  (FROM ("0".."9"|"Z")^SIZE(13)),
    notAfter  [UNIVERSAL 23] VisibleString
                  (FROM ("0".."9"|"Z")^SIZE(13))
}
```

is t p is a co strai d rsio of t `Validity` t p d fi d i X.5 9. co strai ts ar - isibl , i ldi g som compr ssio i t cas of - codi g.

.6 CompactSubjectPublicKeyInfo p

```
CompactSubjectPublicKeyInfo ::= SEQUENCE {
    algorithm        CompactAlgorithmIdentifier
                         {{CompactPublicKeyAlgorithms}},
    subjectPublicKey BIT STRING (SIZE(80..2192))
}
```

is t p is a co strai d rsio of t corr spo di g t p d fi d i X.5 9. si co strai t o t bit stri g, il ot a limitatio i a practical cas , is - isibl a d i lds som compr ssio i t cas of - codi g.

.7 CompactExtension p

```
CompactExtension ::= SEQUENCE {
    extnId    EXTENSION.&id ({CompactExtensionSet}),
    critical  BOOLEAN DEFAULT FALSE,
    extnValue OCTET STRING
} (CONSTRAINED BY {-- Shall contain a value of type
   -- EXTENSION.&ExtnType for the extension object
   -- identified by extnId --})
```

EXTENSION obj ct class is import d from X.5 9. CompactExtension t p is q i al t it t corr spo di g t p d fi d i X.5 9, c pt for t fact t at do ot r q ir t al i sid t extnValue OCTET STRING to b - cod d. is gi s a opport it for mor ffic t codi gs of pro-pri tar t sio s.

. t r g p c

abl s o s r s lts t at r obtai d aft r p rim ts it t c rtificat t p d fi d i t pr io s s ctio , tog t r it a compact t sio for X9.6 compatibilit (s [3] a d pp di).

. e fica e e f e a e f he CompactCertificate e

	4 b RS ce fica e	b ce fica e
P R e c d g	b e	8 b e
D R e c d g	85 b e	4 b e

c rtificat s s d i t is p rim t r cr at d i t follo i g ma r:

32-bit c rtificat s rial mb r;
sta dard algorit m id tifi rs;

“compr ss d” p blic s (c.f. [ ]); a d
“compr ss d” p blic s (c.f. [27]).

rtificat s r sig d it a corr spo di g to t s bj ct’s p blic (63 bit or a 24 bit). ct al al s of ampl c rtificat s ma b fo d i pp di (i t al otatio d fi d i [23]).

compariso of t s c rtificat si s it similar c rtificat s i t X9.6 proposal s o s, ot s rprisi gl , t at X9.6 c rtificat s ar small r (appro ima-t l 6 b t s i t cas a d 95 b t s i t cas). ast majorit of t is (appro . 75%) is d to t s of obj ct id tifi rs to disti g is at-trib t s, algorit ms a d t sio s. s mor i formatio is add d to t t o t p s of c rtificat s, t ill gro at ro g l t sam rat , o r. or mor i formatio abo t t is, s [3].

cl s s d t r r

a d scrib d a alt r ati c rtificat s ta , g rati g compact c rtifi-cat s. s ta is f ll compatibl it t c rtificat s ta d fi d i X.5 9 3. ompar d to .g. draft of I X9.6 , t s ta do s ot sacrific i -t rop rabilit , b t l rag s o isti g p ri c s a d impl m tatio s. pric for t is is slig tl larg r c rtificat s t a for o -X.5 9 compatibl appro-ac s, b t do ot b li t is diff r c to b a limiti g factor. I partic lar, st d i g t o -goi g d lopm t a d ol tio of storag t c olog , it s ms fairl cl ar t at t is small diff r c ill a o l mi or impact o f t r s st ms. rt rmor , t is storag disad a tag ca b som at r m di d b si g - codi g i st ad of - codi g as ll. If t sig at r is do o t - cod d c rtificat , a c rtificat -proc ssi g s st m ill o l a to r -g rat t - codi g from t - codi g b for sag . It is a i -t r sti g rcis to i stigat o m c or (a d tra c rtificat -proc ssi g cod) t is o ld r q ir .

It ma s m t at t ad a c of t c olog ill ob iat t d for compact c rtificat s, si c lo - d d ic s ill a bot i cr as d storag a d fast r proc ssors. is is ot c ssaril t cas , o r, si c t i cr as d s of p blic t c olog is li l to r q ir t at d ic s stor a larg r mb r of s a d s c rit r q ir m ts ma i cr as t l gt s of t os s.

ompact profil s for c rtificat s for partic lar applicatio s d to b co si-d r d as t os applicatio s ar d lop d. It ma also b s f l to st d som mor radical optio s, s c as i cl di g m ltipl p blic s, ac it its o attrib t s, i a si gl c rtificat . rtificat compr ssio s o ld b a s f l ar a of r s arc for ma ars.

f r c s

a , e fica f D e , S b P g 8
ee g a ab e f h : g e eee g g

¨ a d a a d

S , e a Sec a e S ec fica e face : ca d ca d eade , c e T R , S a e S ed h ge c f d a e De e e , 4

D eh, ca h RS ab , eb a

4 de ag, D g a S g a e a , S 8 , , , g h a a a a ab e a h : e c

5 T D e , e , The T S P c e , T R 4 , a a

, e a , SP e fica e The , g e , T SP , e

d, D S , Pa a e e ed e fica e : b X 8 h ce fica e ec , b S X ee g,

8 R ege , P a e c ca , eb a

R e e a , e e X 5 P b c e f a c e e fica e a d R P fie , T R 45 , a a

P g, The e e ca P c P , P ceed g f RS Da a Sec fe e ce , Sa e, US , a a

e a, e e a g RS d h a P ede e ed P , d a ce g S RYPT 8, S, S ge e ag, c be 8

e , e a , X 5 e e P b c e f a c e e e fica e S a P c SP, T R 5 , e

¨ , X 5 a b e ac e fica e , b S X ee g,

4 RS ab a e , e f he 8 P S h , a a ab e f h : a c a ab c

5

R S a a , XDR: e a Da a Re e e a S a da d, T R 8 , g 5

8 S a e, S a da d , e S a & e De e e , P ceed g f P S fe e ce, T a ada, a a ab e f h : 5 5 4 5 de h

S e a a , e f S T a dh de e fica e ha f ch ca d age, P ed S T ec fica , 8

P, e e ca P c e e T a a e Sec P c S ec fica , e e ca P c , 8

S 5 4 , f a ech g e e e c ec The D ec : de , e a a ga a f S a da d a ,

S 5 4 8, f a ech g e e e c ec The D ec : he ca a e , e a a ga a f S a da d a ,

S 88 4 f a Tech g b ac S a a e S : S ec fica f ba c a , e a a ga a f S a da d a , 5

4 S 88 5 , f a ech g S e c d g e : S ec fica f a c c d g R e R , a ca c d g R e R a d D g hed c d g R e D R , e a a ga a f S a da d a , 5

5 S 88 5 , f a ech g S e c d g e : S ec fica f Pac ed c d g R e P R , e a a ga a f S a da d a , 5

S X 5 , D g a e fica e f he a c a Se ce d : cc a ed Sec e Pa e b ec f he a c a Se ce d , d af d c e , e ca a a S a da d e,

S X , P b c e g a h he a c a Se ce d : he c e D g a S g a e g h DS , e ca a a S a da d e,

8 S X 8, D g a ce fica e f b e, cc a ed, a d gh T a ac e a c a S e , 8 h d af d c e , e ca a a S a da d e, e

S X 8, D g a ce fica e f b e, cc a ed, a d gh T a ac e a c a S e Pa : e e a h X 5 , d af d c e , e ca a a S a da d e, e

mpl mp ct rt c t s

is app di co tai s t c rtificat s s d i t ampl s i ctio 4. c rtificat s ar pr s t d r i t al otatio d fi d i [23].

. mpl CompactCertificate

```
exampleRSACert CompactCertificate ::= {
    toBeSigned {
        version       v3,
        serialNumber  1234567890,
        signature {
            algorithm md5WithRSAEncryption
        },
        issuer {
            {
                {
                    type  compact-certs-at-compactIdentifier
                    value CompactIdentifier :
                       '0123456789ABCDEF0123456789ABCDEF01234567'H
                }
            }
        },
        validity {
            notBefore "990503104300Z",
            notAfter  "990510104300Z"
                },
        subject {
            {
                {
                    type  compact-certs-at-compactIdentifier,
                    value CompactIdentifier :
                       '1234554321123455432112345543211234554321'H
```

```
          ¨  a d    a  a d

            }
        }
    },
    subjectPublicKeyInfo {
        algorithm {
            algorithm rsaEncryption,
        },
        subjectPublicKey '3048024100A0658F...0203010001'H
    },
    extensions {
        {
            extnId compact-certs-ce-ansi-x9-68BasicExtension,
            extnValue 'A0'H
        }
    }
  },
  algorithmIdentifier {
    algorithm    md5WithRSAEncryption
  },
  encrypted '0A0658FCBB9BF8C6A0F66D60B7A554E2...'H
  -- 1024 bit signature
}
```

.2 mpl CompactCertificate

```
exampleECCert CompactCertificate ::= {
    toBeSigned {
        version      v3,
        serialNumber 1234567890,
        signature {
            algorithm ecdsa-with-SHA1
        },
        issuer {
            {
                {
                    type  compact-certs-at-compactIdentifier,
                    value CompactIdentifier :
                       '0123456789ABCDEF0123456789ABCDEF01234567'H
                }
            }
        },
        validity {
            notBefore "990503104300Z",
            notAfter  "990510104300Z"
        },
        subject {
```

```
            {
                {
                    type compact-certs-at-compactIdentifier,
                    value CompactIdentifier :
                       '12345543211234554321123455432112345543 21'H
                }
            }
        },
        subjectPublicKeyInfo {
            algorithm {
                algorithm id-ecPublicKey
                -- parameters namedCurve : c2pnb163v1 (X9.62)
            },
           subjectPublicKey '0307AF69989546...D74880F33BBE803CB'H
        },
        extensions {
            {
                extnId compact-certs-ce-ansi-x9-68BasicExtension,
                extnValue 'A0'H
            }
        }
    },
    algorithmIdentifier {
        algorithm ecdsa-with-SHA1
    },
    encrypted '302E021507AF69989546103D79329FCC3D748...'H
}
```

.3 mpl f CompactExtension

is t sio is d fi d i [3].

```
exampleExtension ANSI-X9-68BasicExtension ::= {
    keyUsage {digitalSignature, dataEncipherment}
}   -- PER encoded, this becomes '0xa0'
```

c r a s c c r c a ps

tl f Hü nl in and o ann s rkl

Se e
e ge ha e a ee 8
D 5 E hb e a
{huehnlein,merkle}@secunet.de

E e a a e d e h a a e
a a e e b ha e a f a g a h e h h a be g a
aded h a e a a f a h h a e ed e e
f e a e S e a e f a g a h e h h a e de
ed a e h e e ha e e a d ha d g b e a
e a e ea f ge a a d e a e e eeded b g
he f a g a h e he ffi e ge aded The ef e he
USPS US P a Se e a ed a f a ba ed d a
g a P [ ] de e e a h e he b e
e ed ab e e e e ed b a g a e d g a g a
e a d a e a e ha d a e de e he e de ee
ha h a a h d e a ea ab e e head fa he
b e f e f g he h ge be f a g a e ea ab e
e ad e ed [ ] a a The ef e a e a a a
e e de e he e a P f e a e a e he a g
e e h e
h h e e d e a a e a e a a h g
e a g h a d ge e a e a a d de e e
a Th be e e e e e e h e F
he e a a h a a effi e e fi a f a a
a e h e be a e e d e eed a a e fi a e d
e e ha h e a e a be a a ha
he a e e de ab e e f he e g a e
a d he e he a he f he a

r c

il ails incr asingl r plac pap r ound ail, t r is still a larg n c ssit for con ntional postal s r ic s and it can not p ct d, t at t l ctronic analogu ill sup rs d con ntional ail ntir l in t futur , caus ails o iousl lack so prop rti s of snail ail. r for it is n c ssar to int grat int rfac s to postal s r ic s into t isting offic co unication n iron nt.

n s all co pani s appl franking ac in s, ic ar issu d postal s r-ic pro id rs ( ). urr ntl all suc franking ac in s ar p nsi sp cial purpos ac in s, r ost of t , or at l ast t s curit co pon nt, a to carri d to a post offic to load d aft r pr pa ing a c rtain a ount

. au gar (d.): ’ 7 pp. – .
◯ pr g r- r ag r d rg

of sta ps. s curit of t is proc dur , i. . t at it is not possi l to forg sta ps, r sts in t s cr c of t int rfac s and tools. n or od rn franking ac in s it int grat d od s to p rfor t loading r ot l r quir a s cur dir ct conn ction to t and so sort of out of and pa nt for t oug t sta ps.

It is cl ar t at it ould d sir a l to us isting offic co unication co pon nts, lik ulti purpos print rs and s it conn ction to t int r- n t to r plac t p nsi sp cial purpos franking ac in s and a oid t anno ing trip to t post offic . ut p rfor ing t loading proc ss ia op n n t orks lik t int rn t and using standard p rip rals to produc and print sta ps id ntl ars so risks. H nc it is n c ssar to int grat s curit c anis s ic pr nt unaut ori d loading of t franking ac in and forging or cop ing of sta ps.

r for t initiat d t infor ation as d indicia progra [ ]. In t is conc pt t aut nticit of sta ps is nsur d , or signatur s, ic ar cod d in a t o di nsional arcod and print d as part of t sta p on a l tt r for a pl . n a l tt r arri s at t t sta p is scann d and t signatur is c ck d aft r o taining t c rtificat fro a di- r ctor . caus on as to conn ct to a possi l r ot dir ctor s r r to look up t c rtificat to rif t signatur t is st p is c rtainl t ottl n ck in t rification proc dur . it curr nt t c nolog it s s i possi l to c ck a non-n gligi l fraction of t ug a ount of l tt rs. naut ori d sta ping is pr nt d using sp cial purpos ard ar at t cli nt s st . caus cop ing aut ntic sta ps can not pr nt d it is n c ssar to int grat data c ararct ristic for t l tt r lik t ip-cod , t adr ss of t r c ipi nt and t dat into t sta p. us, cop ing sta ps onl ak s s ns in circu stanc s r on n ds to s nd an l tt rs it id ntical c aract ristics. possi i- lit of cop ing sta ps can furt r r strict d li iting t ti of alidit . Ho r, on can still i agin situations r ill gal duplication of sta ps a a conc rn. r for it ill n cc sar to log t rifi d and un pir d sta ps.

s not d a o t application of digital signatur s and acco pani d pu lic k infrastructur s introduc s an unr asona l o r ad in t rification st p. caus t signatur s ar clusi l c ck d t it is cl ar t at on a as ll us s tric algorit s it d ri d k s to o tain t sa s curit f atur s. is alt rnati approac , ic is discuss d in t is ork, ill allo to c ck all arri d l tt rs during t sorting proc ss. urt r or ill s t at t sp cial purpos ard ar d ic it r alti clock is not n c ssar . H nc it ill uc c ap r to i pl nt our conc pt co par d to [ ].

is pap r is organi d as follo s: In ction 2 ill ri fl plain t c ntral f atur s of 's infor ation as d indicia progra [ ] and point out t d fici nci s for road application. In ction 3 ill introduc our approac using s tric algorit s and g n ral purpos s art cards.

. r i us rk

r a n s ral pu lications tr ating t r ali ation of s cur l ctronic sta ps. In [2] astor outlin s o suc a s st ig t ork. In [3] gar and Y gi a d tail d discussion of t r quir nts and possi l solutions, ut in contrast to our conc pt t onl consid r prot ction digital signatur s. urt r or t r is a pat nt application on cr ptograp icall s cur d l ctronic franking s st s [4].

2 ’s r a as c a r ra ( )

In ord r to facilitat l ctronic franking and pr nt fraud t initiat d I I [ ]. In t is progra t aut nticit of an infor ation as d indicia (l c- tronic sta p) is nsur d appl ing cr ptograp ic c anis s to data ic ar r lat d to t pi c of ail und r consid ration. In t follo ing ill ri fl ig lig t t ain issu s of I I and point out t pro l s for larg scal application.

2. ri r i I I

r custo r o is illing to us l ctronic sta ps u s a *s a* *i* *i (* as sp cifi d in [, art]. is d ic is a sp cial pi c of cr p- tograp ic ard ar it r al ti clock, ic can conn ct d to t parall l port for a pl . ” or s curit r asons, t ill <u>not</u> a g n rali d digi- tal signatur d ic .” [, pag -4]. or t pri at k in t t cr at s a c rtificat containing t corr sponding pu lic k , ic is stor d in a c rtificat dir ctor . can load d it a c rtain a ount of sta ps, conn cting to t and trigg ring so sort of pa nt c anis for t sta ps. load d is t n us d to issu l ctronic sta ps ic ar cod d in a t o di nsional ar cod and print d on t l tt r. sta p as sp cifi d in [, art] consists of 49 t s l tt r sp cific data (.g. custo r I , dat of ailing, d stination, postag , s rial nu rs, ...) and a digital signatur of t s data ic is g n rat d t using its pri at k . allo d signatur c anis s and k si s ar 24 it , 24 it or 6 it - . us t si of t ac in r ada l sta p is 77 t s for or 9 t s n using -t p signatur s. H nc on as t c oic t n a arcod d sta p of r asona l si ( ) or ffici nt rification ( ). part of t progra ic is not t sp cifi d in [ ] is t rification proc - dur at . is rification st p ill n d to consist of r ading t arcod d sta p, conn cting to t dir ctor and rif ing t signatur . It is cl ar t at t r ill illions of l tt rs ic a to andl d t r da . us it is cl ar t at for p rfor anc r asons it ill not possi l to rif r sta p. is a l ad to ”calculat d” fraud.

2.2 u ri i I I ’s r l s r r c l pplic ti

In t is s ction ill ri fl su ari t ajor pro l s of I I for larg scal application:

– I I r quir s sp cial purpos ard ar ic l ads to ig r initial costs and nc a d t r pot ntial custo rs.
– arcod ic carri s t sta p is r lati l ig ic l ads to pro l s n sta ping r gular l tt rs or postcards.
– n using -t p signatur s on o tains s all r signatur s and arco-d s ut as to p rfor a l ss ffici nt rification proc dur .
– In ot cas s (, -t p) on n ds to look up t c rtificat in a dir ctor , ic ak s t rification proc dur in ffici nt and ak s t rification of all sta ps i possi l .

r as a c p a rac ca a c r c r c a ps

In t is s ction ill introduc a a to r ali l ctronic sta ps ic sol s t a o pro l s it out r ducing s curit . In contrar our approac allo s uc or ffici nt rification and nc ak s t rification of all sta ps possi l ic s ould l ad to n l ss fraud. In our conc pt assu t at r custo r as acc ss to a quip d it a print r, a s art card r a-d r and an int rn t conn ction. It is id l li d t at it in a f ars s art card r ad rs ill co standard for s. urt r, t issu s to all custo rs, o ant to us l ctronic sta ps a d dicat d soft ar , call d t sta p progra , and a s art card. ac s art card as i pl nt d a s -tric ncr ption function F and as s cur l stor d a distinguis d s cr t k . is s cr t k is d ri d fro a ast r k of a local offic (.g. for r ZI -cod) and t custo rs I using an ar itrar s cur as function h or alt rnati l a s tric cip r in as - od . urt r, ac s art card as 2 int rnal count rs z and z , ic cannot acc ss d fro t outsid . ik in t approac of our s st consist of 3 stag s: arging t s art card, n rating sta ps, rification of t ut nticit of t sta p t .

. r i t rt r

for a custo r can cr at l ctronic sta ps, as to c arg is s art card. is is initiat d s nding t co and _ tog t r it t a ount x to t s artcard. s art card incr nts t int rnal count r z and using its s cr t k to co put t ncr pt d c arg r qu st. is r qu st contains t count r z , t a ount x, t custo rs I and t k ord - . n t sta p progra s nds t is r qu st to t local offic (.g. ia ail, ttp, tcp).

ft r r c i ing t is r qu st, t d ri at s t custo rs s cr t k fro its local offic k (ic its lf a d ri d fro a glo al ast r k) and d cr pts t r qu st, t r rif ing its aut ntic . If positi , t us s t custo rs s cr t k to g n rat an ncr pt d c arg co and containing t count r z , t a ount x and t k ord and s nds it to t custo r.

inall t custo r for ards t r c i d ssag to t card, ic d - cr pts t c arg co and. If t c arg co and is rifi d t card incr - nts its count r z x.

. custo r s nds (_ , x) to t card.
2. card s ts $z = z +$ and s nds $Y := F$ (, z , x) to t custo r.
3. custo r s nds $(Y, ID$) to t .
4. co put s $SK = h(SK , ID)$ and (, z , x) $=$ F^{-} (Y).
. s nds $Z := F$ (, z , x) to t custo r.
6. card rifi s F^{-} $(Z) =$ (, z , x). If t is is ok it s ts $z =$ $z + x$.

.2 r ti t ps

n a custo r ants to sta p a l tt r, us s is sta p progra to s nd a sta p r qu st containing t postag a ount y (ic can d t r in d t sta p progra), a as alu v of t sp cific para t rs of t l tt r and t k ord to t s art card. sp cific para t rs of t l tt r contain t addr ss of t r c ipi nt, t custo rs I , t dat and a contain ot r data as ll aking t sp cific para t rs uniqu . ot t at t custo r is r sponsi l to us t corr ct dat . If t dat is not it in a sp cific ti fra n c ck d at t t l tt r is consid r d or clos l , as it ig t a a fraudul nt sta p. us if t dat is not corr ct t l tt r ill tak long r ti to d li r d. card c cks z y and, if positi , d cr nts z y and g n rat s t sta p for t l tt r, ncr pting v concat nat d it y. If $z < y$ t card r turns .

inall t sta p and t sp cific para t rs of t l tt r ar print d onto t l tt r using an ar itrar ac in r ada l ncoding.

. custo r d t r in s t postag a ount y and t sp cific para - t rs of t l tt r D, calculat s $v := h(D)$ and s nds (, v, y) to t card.
2. card c cks y z . If positi , it s ts $z = z - y$ and s nds $X :=$ F (v, y) to t custo r. If n gati , it s nds .
3. custo r prints (D, X) onto t l tt r.

. ri c ti t li it t ps t

can rif t alidit of sta ps it out conn cting to a data as for r sta p. irst it c cks t at t sp cific para t rs ar consist nt it t l tt r (.g. t at t addr ss and t dat is corr ct). If t dat is not it in a c rtain ti fra (i. . dat d in t futur or old r t an (sa) t r da s) t r dir cts t l tt r to a plac r sta ps ic ig t a n forg d ar consid r d or clos l . nl in t is cas t stor s t suspicious sta ps in a data as to r cogni copi d sta ps. ot t at t custo r its lf is r sponsi l for t dat in t sta p to allo ti l proc ssing it out s cond l l c cking. is strat g ak s t pr s nc of a s cur r al-ti clock at t cli nt s st o sol t . ft r t is c cking t co put s t custo rs s cr t k using t s cr t k of t local offic and t custo rs I contain d in t sp cific para t rs of t l tt r. sing t custo rs s cr t k t d cr pts t sta p i lding a pair (v, y). inall , it c cks, t at a ount y is suffici nt as postag for t is l tt r and t at v is t as alu of t sp cific para t rs of t l tt r.

. r ads (D, X) and c cks t consist nc of D (.g. consist nc of addr ss, piration of alidit).
2. tracts ID fro D and co put s $SK = h(SK \;, ID \;)$.
3. co put s $(v, y) = F^{-} \; (X)$.
4. rifi s $v = h(D)$ and c cks t at a ount y is suffici nt as postag .

. pl t cti

lt oug a sta p is tig t to a fi d s t of c aract ristics of t l tt r, on still as to consid r r pla attacks. It is not unlik l t at a co pan n ds to s nd an l tt rs it t sa c aract ristics it in a s ort ti (.g. t corr spond c it on of its d p nd nci s). In t is cas t co pan could sa a lot of on ill gall cop ing and r using sta ps.

onl a to d t ct ill gal cop ing is to log all rifi d sta ps in data- as s. inc ail is usuall rifi d at a post offic locat d in t sa r gion as t costu r, t is can don in a d c ntrali d a , i. . t sta ps of a c rtain costu r ar logg d at t r gional post offic . data of ail ic is rifi d diff r nt post offic s can c ang d n t ork conn ctions.

urt r or , sinc sta ps ar lik l to rifi d in ss ntiall t sa ord r as t a n g n rat d, t logging can don r spac ffici nt: or ac costu r C l t i t gr at st nu r i for t at all sta ps of costu r C a ing s rial nu r s all r t an i ar it r pir d or a n alr ad rifi d. n for ac costu r C it is suffici nt onl to stor i and t (co pr ss d) list of t s rial nu rs gr at r t an i of t rifi d sta ps fro costu r C.

or concr t sti at s for t p ct d si of t data as s r f r to [3].

4 c s

ill conclud t is ork ri fl co paring our approac to I I :

t s I I

– If a s cr t k *SK* of a local post offic is co pro is d in our approac t as to r plac a s t of s art cards – all s artcards os k is d ri d fro *SK* . In I I , if a s cr t -k as co pro is d, on ould onl n d to r plac t c rtificat s sign d t is k . is is no r al t r at as *SK* and t s cr t -k ar additionall s cur d strict organi ational ans.
– using t sp cial purpos ard ar it r al-ti clock it ould ard r for an attack r to c ang t ti to produc forg d sta ps.

t s ur ppr c

– ur approac do s not r quir sp cial purpos ard ar ut si pl s art cards at t cli nt ic is uc or cost ffici nt.
– ”signatur ” in t sta p in our conc pt is at ost 6 t ic is l ss t an alf as ig as in I I using -t p signatur s, not to talk a out . us our sta ps ar no pro l s n if print d to postcards or s all l tt rs. us our sta ps do not caus pro l s, n if t ar us d for postcards or s all l tt rs.
– rification of sta ps in our approac is uc or ffici nt t an in I I , caus on do s not n d to conn ct to a dir ctor to o tain c rtificat s, ut d ri s t corr sponding s tric k si pl op rations. us it ill f asi l to rif all sta ps, r cogni forg d sta ps and nc pr nt fraud.

o paring t argu nts for I I and our approac t ink t at our approac is uc or suita l to i pl nt a larg scal s st for l ctronic franking.

r c s

U ed S a e P a Se e: *r r an ri ria r in r a i n- as in i ia an s ri ar hi r r s ag ring s s s* g h 8 a h : b
é Pa Y *( ) ni rsa in r a i n as ran ing s s r a a ai r ssing* a f g : 4
D T ga a d e e Yee *r gra h 's n j s r r ni ai an r* Te h a Re U S S h f e S e e a ege e U e P b gh
4 d e e a P e ga a e a a a U de he Pa e e a T ea P T *s an h r r ri ing s ing an rin ing s ag in i ia n n s* e a a a be : 4 h

pl l r r r

a a o

& Re ea ch ab a e a
4- - a a a ae a a a -8555 a a
sako@ccm.c .nec.co.jp

t t. Th a e e e he e e a f a g a e e e The a f h e e ffe a c e ha a g f e ca ag ee be a The e e a e efi e a a a e e a c a e ha e a e f c e
h e he che e e g a h c f e f ec ee he c e a a c ca e ac a e a a e e effec he ea e f ac a e

e fa e a c e e a ha h f c

r c

id spr ad s of digital t or s as cr at d a i d of c b r-soci t os citi s ar i cr asi gl abl to participat i t f ll ra g of acti iti s associat d it a r al co it . co i c ic t still app ar to lac , o r, is a a d s st for dra i g lots. I a r al co it , a gro p of p opl ca gat r i o plac to dra lots b t s l s or to obs r t at a r pr s tati i d d dr i a fair a r. i g p sicall pr s t is ss tial to b ass r d of fair ss, i. ., t at t r as o c ati g i t proc ss, b t t is is ss tiall i possibl i a c b r-soci t .

r ptograp ic protocols pro id a t or tical basis for ac i i g ass r d fair ss, a d st di s o s c r lti-part co p tatio d o strat t possibilit of d t r i i g a i r ra do l [,2]. oldsc lag a d t bbl bi pr s t a si pl lott r sc bas d o a d la i g f ctio [3]. s sc s ca b s d i pri cipl to b ild a lott r s st , gi t ir sp ci catio s. Ho r, a act al tool to s pport a fl ibl , *i rs l* lott r , os d sig a d p rpos s ig t b odi d, as, to t a t or's b st o l dg , t to b r port d.

is pap r pr s ts t i pl tatio of a co i t digital lott r s r r to b s d o t . It off rs a o tco t at a gro p of s rs ca agr to a b d t r i d ra do l . s r r a b s d for s l cti g at ra do a si gl i i g participa t or ltipl i rs at ario s l ls of i i g, (.g. a si gl st pri i r a d 2 d pri i rs, tc.) It ca also b s d for t ra do ord ri g of participa ts (.g. to d t r i a dra for a at l tic

. au gar (d.): ' , 7 , pp. – , .

co p titio .) s r r allo s a i itiator of a lott r s ssio to d t r i its p rpos a d d sig its r l s.

I d sig i g s c a lott r s r r, s c rit r q ir ts a d applicabilit f at r s oft co i co flict it ac ot r. a car f ll d sig d t lott r sc t at t s r r adopts to t t follo i g r q ir ts fro t asp ct of bot s c rit a d applicabilit .

ir ss s rs ca b ass r d t at o tco s ar g rat d i a fair a r, d r r aso abl ass ptio .
ri ilit s r r pro id s s rs it ri catio a s to d t ct a i co sist ci s ad d ri g t s ssio .
i li it r r s ro d co pl it of t sc is pt as lo as possibl .
st ss s r r do s ot fail to co d ct a o tco , i t pr s c of la pla rs, i. . t os o for so r aso fail to participat as t s o ld.
l i ilit s r r ca a dl a t p s of lott ri s t at o ld b carri d o t i g ral.
s ri ti s r r pro id s a si pl t plat b ic t i itiator ca d scrib i d tail t c aract ristic of t lott r d sir d.
li g r lit co sid ratio st b ta i d sig i g appropriat a -i t rfac to i cr t a s s of r alit " to t act of participa-tio .

b li t s co str ct d lott r s r rs ill b s f l o t I t r t i a b r of a s: a i di id al ig t s o , for a pl , to c oos fro fri ds distrib t d o r t t p rso s to o to gi spar o i tic ts; a ag rs of p blic faciliti s ig t s o to c oos a o g applica ts for s of t os faciliti s; l d lop d l ctro ic a ctio s st s or l ctro ic oti g s st s ig t s o to old a lott r i cas of a ti ; tc.

r st of t pap r is orga i d as follo s: i ctio 2, d scrib t basic proc ss i ol d i a lott r s ssio , a d i ctio 3, pr s t t i pl tatio or sp ci call .

r c

lott r sc t at a plo d i ol s t o i ds of s rs: a *l r*, o i itiat s a lott r s ssio o t lott r s r r, a d *l rs*, o acc ss t s r r a d participat i t lott r s ssio .

t ot r a d, t lott r s r r a ag s a d carri s o t ltipl lott r s ssio s i itiat d b t s rs. or sp ci call , t tr st ort s r r:

pro id s s rs a a s to start lott r s ssio s a d b co d al rs,
ai tai s t s cr c of i itial al s of ac s ssio til its clos r ,
pro id s s rs a a s to participat i s ssio s t is to particpat i , o a d dat , c t s a lott r a d co p t s its o tco , a d
displa s t o tco of ac c t d lott r s ssio i a ri abl a r.

. ut

o tli of o a s ssio proc ds is as follo s:

. d al r i itiat s a lott r s ssio o t lott r s r r. H d scrib s its d sig a d p rpos si g a t plat , t d t r i s a i itial al x a d s b it it.
2. s r r, o acc pti g t r q st, d t r i s a s r r's i itial al y for t s ssio si g a ra do b r g rator. s r r assig s a iq s ssio I *sid*.
3. s r r adds to a s ssio list t d scriptio of t s ssio , ic is p blis d o t b, tog t r it co it ts of t d al r's i itial al x a d t s r r's i itial al y. H r , t co it ts ar co p t d as $H(sid \circ x)$ a d $H(sid \circ y)$ si g a cr ptograp icall s c r as f ctio [4], H.
4. ac pla r i c oos s t s ssio is to participat i , a d rolls is a tog t r it a stri g r fr l cr at d b i s lf.
5. t dat of c tio , t s r r co p t s t o tco fro t o i itial al s a d stri gs cr at d b ac pla r. r s lt of t s ssio is app d fro a as d al $H(x \circ y \circ r \circ \cdots \circ r \circ DESC \circ sid)$, r $DESC$ d ot s a stri g iq l co rt d fro t d scriptio of t s ssio
6. o tco is p blis d o t b, tog t r it d cr pt d i itial al s x, y a d stri gs r cr at d b ac pla rs.
7. ac pla rs a rif t follo i g: t stri g as cr at d is i d d i cl d d, t o tco as b corr ctl co p t d, a d t i itial al s ad b corr ctl co itt d, b co p ti g $H(x \circ y \circ r \circ \cdots \circ r \circ DESC \circ sid)$, $H(sid \circ x)$ a d $H(sid \circ y)$.

. tur s

ass t at a cr ptograp icall s c r a d id al as f ctio ac i s t follo i g prop rti s:

- *ss.* i $H(x)$, it is ard to co p t x. or o r gi $H(x)$ a d a partial stri g co stit ti g x, it is ard to r co r x tir l .
- *llisi -r .* It is ard to d x a d x t at i lds $H(x) = H(x)$.
- *r l l.* istrib tio of $H(x)$ ca b r gard d as ra do .

as d o t prop rti s of t as f ctio , t lott r sc d scrib d abo pro id s t follo i g f at r s:

tri gs c os b t pla rs *q ll* co trib t to co p ti g t o tco . o tp t of a id al as f ctio is d p d t o ac bit of t i p t. o trolli g a part of t i p t ca ot co trol t o tp t.

---

he e e a e a e he a e f he ea e a a e a a eg a be f each a c a he he ha h f c

la rs ar ot allo d to gai a fair ad a tag . I ord r for a pla r to s l ct a stri g ad a tag o s to i s lf, o l dg of all t ot r pla - rs'stri gs a d i itial al s x a d y ar r q ir d. Ho r, p blic i for a- tio r gardi g x a d y is $H(sid\circ x)$ a d $H(sid\circ y)$, ic l a s o i for atio o x a d y d to t o - a ss of t as f ctio . if a pla r col- l d s it t d al r, t al of y is r l a d b o d t tr st ort s r r.

it r d al rs or t s r r ca alt r t i itial al s it o t b i g d - t ct d. I ord r to alt r t i itial al x b x , or y b y , $H(x) = H(x\ )$ or $H(y) = H(y\ )$ st old if ot d t ct d. s collisio s ar ard to d d to t collisio -fr prop rt of t as f ctio .

. cur t c t Its st

possibl co c r i t propos d s st is t c trali d po r at t s r r, i. ., it o s all t i itial al s of t s ssio s. a to d c trali its po r is to p so of t s al s fro t s r r a d distrib t t a o g a d al r a d/or so of t participa ts at ac s ssio . or a pl , a d al r a ot s b it its i itial al x i plai t t i itiati g a s ssio , b t i st ad s b it $H(sid\circ x)$ fro t b gi i g. s t s r r is pr t d fro o i g x. t participa ts, so or all of t , ca ol taril act i s tti g i itial al s. at is, t ca s d t as d al of a stri g of t ir c oic , ic ill b p blis d, b for t s ssio b gi s. ill r al t stri g o l aft r t closi g of t s ssio . I t is cas , ac participa t ca b co pl t l ass r d of fair ss, b ca s o c ati g is possibl as lo g as ps t stri g to i s lf.

bigg st dra bac to t is approac is t at bot d al r a d ol t r participa ts st b a ailabl co p ti g t o tco . is aff cts t sc 's rob st ss, t at t s ssio a t r i at it o t a o tco .

f l t at a or s itabl approac is to i trod c ltipl i d p d t titi s it i a s r r, o is al a s ass d to b pr s t i c ti g a lot- t r . i itiati g a s ssio , ac tit g rat s a i itial al a d broadcasts its as d al to ot r titi s. s t of all as d al s ca b co sid r d as t s r r's as d al s, or or co i tl , t as d al of all as- d al s fro t titi s ca b s d. is i pro t do s ot ca s a c a g i s r proc d r . t r co tio al t c iq s o t r s old sc s ca also b plo d.

l r r r

a co str ct d a lott r s r r o ic to i pl t t propos d sc .

or t i pl tatio , a sp ci call d sig d:

a t plat ic allo s a d al r to d scrib t d sig a d t p rpos of is lott r , a d

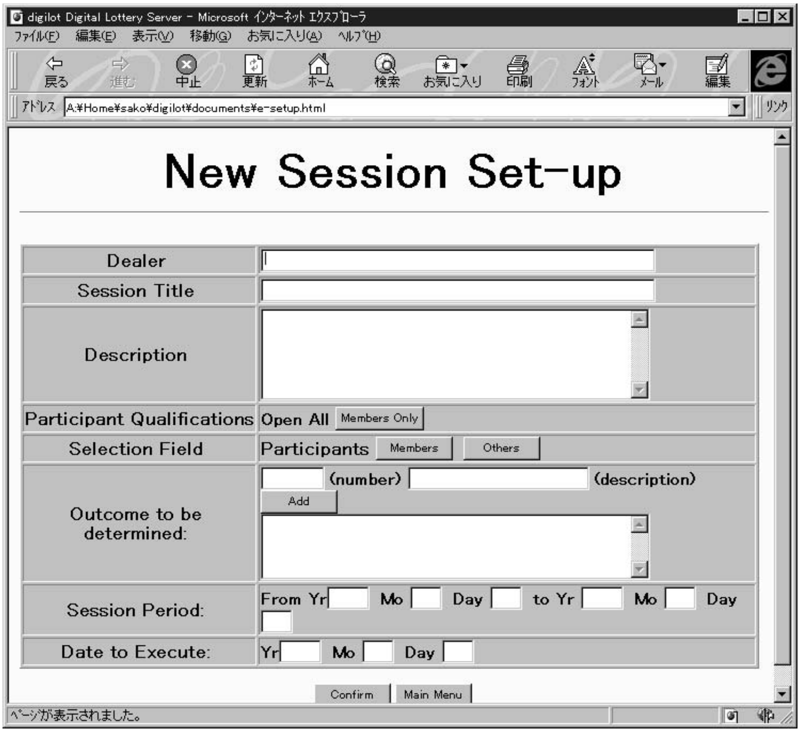
a lott r gi ic sp ci s t i p t to t as f ctio a d appi g of a as d al to t o tco of t lott r .

. . a Page f e Se e

t rt s ss
d al r, t p rso o op s a lott r s ssio , sp ci s t follo i g si g t t plat :

t titl of t s ssio
t ai of t s ssio
participa ts' q ali catio s
ssio s a b it r op all or li it d to b rs. I t latt r cas , a list of b rs st b gi .
s l ctio ld
l ctio s ca b ad fro a ld co prisi g participa ts, li it d - b rs, or ot rs.
I t t ird cas , a list of it s i t s l ctio ld st b gi , for a pl , spad s, arts, cl bs, or dia o ds for a card ga , or -6 for a dic ga .
s co d cas appli s o ds to s l ct a o g t b rs it q al probabilit , d spit possibl *laziness* of ac b r. at is, if a b r fails to participat , still as a c a c of i i g (or, si ilarl , losi g) i t lott r .
o tco to b d t r i d: its it d scriptio a d b r.
It s ca b pl ral, .g. o st pri i r a d 2 d pri i rs.
op i g a d closi g dat s
dat to c t lott r
a i itial al x

lt o g t is t plat do s ot s r to r pr s t all t p s of possibl lott ri s, b li it co pactl d scrib s ost of t d sig s a d p rpos s of lott ri s.



. . S a g f a e e Se

a r q st for a lott r s ssio it its d scriptio is s b itt d, t s r r as s t d al r to c oos a i itial al x. s r r t g rat s a ra do stri g y to b t s r r's i itial al for t at s ssio , a d assig s a s ssio b r (s ssio I , sid). d scriptio of s ssio it al s of $H(sid \circ x)$ a d $H(sid \circ y)$ is p blis d o .

rt c p t s ss

ac participa t sp cif a s ssio b r, it r o obtai d fro a list of p blic s ssio s, or o pro id d b t d al r or a ot r participa t. s r r displa s t ai a d d scriptio of t s ssio , tog t r it as d al s $H(sid \circ x)$ a d $H(sid \circ y)$. t pi g i is a a d a fr l c os stri g, co pl t s t participatio proc d r .

---

f a fe e be a e a c a e he ee e e a ec e a h ch f e b he e e bef eha

acc pti g is tr , t s r r displa s is r gistratio b r it t stri g as s b itt d.

su t f s ss

ft r t closi g dat , t lott r s r r co p t s t o tco a d p blis s t r s lt. s r r pro id s a ri catio tool so t at all participa ts ca rif t at t r s lt is co sist t it t sp ci d proc d r . tool also allo s s rs to dit a i p t to t o tco -co p ti g f ctio . s o ca obs r o a alt r ati c oic of is stri g o ld a c a g d t o tco .

p c c t f t tt r

follo i g ar i p ts to t lott r gi :

d al r's a
d al r's i itial al a d its p blis d as d al
s r r's i itial al a d its p blis d as d al
ac participa t's a , is r gistratio b r, a d is stri g i t ord r of participatio
a list of it s i t s l ctio ld i a sp ci d ord r
a list of o tco d scriptio s a d t ir b r i t a o c d ord r s ssio I

gi co cat at s t abo i p t i t sp ci d ord r a d co p t s its as d al . as d al is t app d to a b r i a list of s l ctio ld it s si g od lar co p tatio . ltipl it s ar to b s l ct d, t as d al s ar s q tiall as d to obtai c ssar disti ct i i g it s.

I p t t t s

a i pl t d a d o stratio s st ic or s o i do s 95 a d i do s s r r/ or statio it ti H . s st r q ir s a bs r r s c as rso al bs r r or I t r t I for atio r r, a d a tscap a igator. progra is ritt i a d as 6 li s, l ss t a a t t of ic is d ot d to d scrib t lott r gi . or act al s , ar also d lopi g a s st t at s s racl databas for t s ssio a ag t, it - ail s r ic s for s rs to otif t stat s of o 's lott r s ssio .

cl r s

I t is pap r, a pr s t d t d sig a d i pl tatio of a lott r s r r o . is is a act al tool to s pport a fl ibl , *i rs l* lott r ,

The c e e a e e fie a g he e b he e- a a e e g e e fica e f g a g a e ech e a a e

r a s r ca d a d start a lott r s ssio of is p rpos . s r r pro id s s rs a ri catio a s, ic lps t to b ass r d of fair ss. ro g t s of a tr st ort s r r t at ai tai s s cr ts, t sc do s ot co plicat act al op ratio s or ad rs l ff ct t as of act al s .

r c s

a e *i li i g l h I* age 8

e e ch S ca a g e *t l t l k r* age 8 8

Da ch ag a S a S bb eb e *u li l rifi l tt ri s li ti s f l i g u ti s i i l r t gr h* 8

4 D g a S *r t gr h – h r r ti –* R P e 5

5 R a R e *l tr i tt r i k ts s i r m ts i i l r t gr h*

a h e Y ha a a chea Rab *tt ri s ith iqu i rs I ur l is r t th m ti s* 8 - 8 5

r ’ r c s s
l c r c l r c r c r

a i r op , to io a a, a d ua . rt ga

e Sc e ce De a e , E T S ge e a f a ca
U e a e a aga, a aga SP
{jlm, amg, juanjose}@lcc.uma.es

c P b c e f a c e a e c e e he ba f he c a ee e g a a ee he ec e a e f e e e a ca e e ec c c e ce, g e e c e e a h a g a b Th a e ce a e f a c e e g , e e , a e a age e a ce fica e ha ba e he c e f he e ec c a e ce a he c e f ea ce fica e e e ec e ea e f e a b e he b c e ce fica e , e ha ce he effic e c f e ca ce e , a a ca ab a ch a b e The e , e e e a e e a he U e f a aga, a ece e ec e b Re R S, he a a Re ea ch a ca e c e S a , e he b c e e ce f ec e e ec c a

I r c

r is id agr m t o t imm s pot tial of I t r t, sp ciall for cit- i g applicatio s lik l ctro ic comm rc , go r m t-citi r latio s ips a d digital distributio , but a sig ifica t part of t us rs ar still r lucta t to us t t ork for fi a ciall or l gall s siti data du to t lack of s cu- rit . gro t a d p rforma c of I t r t ar ad rs l aff ct d b s curit issu s a d b t op d sig of t t ork its lf. us, d spit its ormous possibiliti s, t I t r t as ot t b com a commo icl for t os appli- catio s b caus it is still too as to i t rc pt, mo itor a d forg m ssag s, a d imp rso at us rs [ ].

ral s st ms, suc as *rb r s* [2,3] a b propos d to prot ct commu- icatio s o r public t orks usi g s mm tric-k cr ptograp . os s st ms ar ot asil scalabl for larg groups of us rs b lo gi g to diff r t orga i ati- o s. Ho r, som fforts a b accomplis d to sol t is probl m [4,5,6].

t ot r a d, public-k cr ptograp [7] s ms to b ll suit d to satisf t r quir m ts of t I t r t, a d is fast b comi g t fou datio for t os applicatio s t at r quir co fid tialit a d aut ticatio i a op t ork.

id spr ad us of a global public-k cr ptos st m is compl m t d b a *bli* - *Infr s r r* (KI), a ffici t a d trust ort m a to ma ag

. au gar (d.): ’ , 7 , pp. – , .
◯ pr g r- r ag r d rg

public-k alu s. KI is a ital l m t b caus it abl s t applicatio of t cr ptos st m to t c a g of s siti i formatio b t parti s t at do ot a a fac to fac i t ractio .

is pap r i troduc s rt' , a k ma ag m t a d c rtificatio s st m bas d o t l ctro ic mail s r ic structur , a d it is orga i d as follo s: s ctio 2 pr s ts t s st m structur a d op ratio ; s ctio 3 summari s additio al f atur s t at impro t ffici c of t s st m; s ctio 4 d scrib s t protocol us d to acc ss t k s r rs a d, fi all , s ctio 5 pr s ts co cludi g r marks.

scr p f s

fu dam tal pri cipl s of rt' ca b summari d i t follo i g d sig goals:

- to us a s arc it ctur t at satisf t ds of ar-c rtificatio so t trust ca b bas d o at r crit ria is us d i r al lif ;
- to limi at probl ms associat d it t r ocatio proc dur s a d simplif t alidatio of c rtificat s;
- to a oid arc it ctur s t at i ld scalabilit probl ms;
- to a oid t s c ro i atio probl ms associat d to sc m s t at k p multipl copi s of t k s a d c rtificat s; a d
- to mi imi t t ork traffic, sp ciall t at g rat d b ma ag m t op ratio s.

. r c r

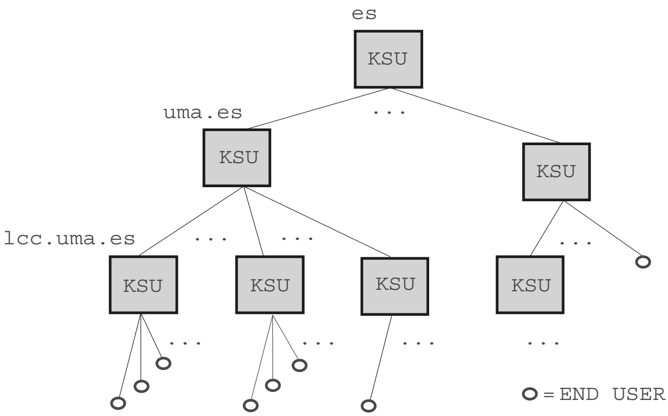
mai l m t i t i rarc is t *s r i ni* (K), ic i t grat s bot k c rtificatio a d c rtificat ma ag m t fu ctio s. rt' us s a sc m it arious K s op rati g o r disjoi t groups of us rs, co formi g a pr d fi d i rarc .

igur s o s t s st m structur . K i rarc d fi d b rt' is parall l to t i rarc of I t r t domai s. r l a t f atur is t at K s ar associat d to t corr spo di g -mail offic s.

s s o i figur 2, r K is ma ag d b a *r ifi i n h ri* ( ). dditio all , it co tai s a *b s* to stor t c rtifi d k s of its us rs; ac us r public-k c rtificat is stor d clusi l i t databas of is/ r K . t ird compo t i t K is t *k s r r*, ic r c i s r qu sts a d d li rs t c rtificat s to t r qu st rs. k s r r also ma ag s a c rtificat cac t at k ps som of t t r al c rtificat s r c tl r c i d.

c rtificat cac , car full d sig d, a c s t ffici c of t s st m it out i troduci g a s curit risk. urt rmor , a ca d fi its o cac polic accordi g to its us rs ds.

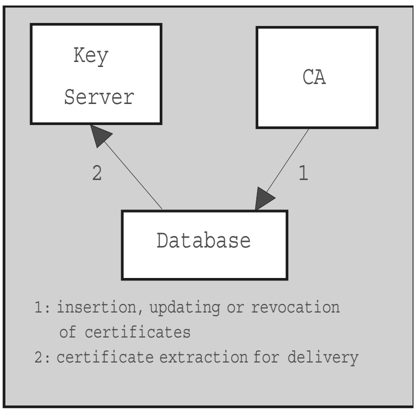
ac ca s t r strictio s to limit t us rs or K s allo d to acc ss t s r r. is f atur pro id s t it a us ful tool to a oid abus a d to bala c t orkload b t diff r t s r rs.



e a ch f e e e

c rtifi d k s ar ma ag d sol l b t corr spo di g ; t r for , k updati g a d r ocatio ar local op ratio s it out i flu c i t r st of t s st m.

must u d rli t at o *r ifi* *i n is* ( ) is us d i t d sig . alidatio of a c rtificat is ac i d usi g t *li i* *n* ( ), a tim stamp stat m t sig d b t att sti g t at t c rtificat as ot b r ok d at t tim of issua c of t . c rtificat is co sid r d *ir* if t alidit p riod as fi is d. If a c rtificat as ot pir d call it a *i* c rtificat . acti c rtificat is *li* if it as ot b r ok d; t r for i ord r to alidat acti c rtificat s t simpl issu s a .



SU e

. s p r i

rt' d fi s a sp cial us r, @ *in* , i r K i ord r to d ot t corr spo d t . c rtificat of a is stor d clusi l i t databas of its par t K . c ptio all , t k of a locat d at a top-l l domai is stor d i t databas of its o K , c rtifi d b t domai r gist ri g aut orit (.g. *I*). K s distribut d b a K ar al a s c rtifi d b t corr spo di g ; t us, i t subs qu t discussio , ill us t t rms 'k ' a d 'c rtificat ' qui al tl .

logical structur of t data tra smitt d b a K i r spo s to a c rtificat r qu st is importa t i ord r to clarif t k distributio proc dur . c rtificatio r spo s co sists of t o compo ts:

- a .5 9 3 c rtificat [ ] co tai i g, amo g ot r i formatio , a s rial um-b r a d t p ct d lif of t c rtificat (t alidit i formatio);
- t sig d b t , co tai i g t c rtificat s rial umb r a d t tim of issua c .

t r s st ms, lik *I/* *I* [9,], propos a similar m c a ism call d *n - i r li i n* ( ). ut for our purpos s t is solutio is ot co - i t b caus it do s ot pro id tools to limit t us of t at "pr - alidat d" c rtificat i t futur .

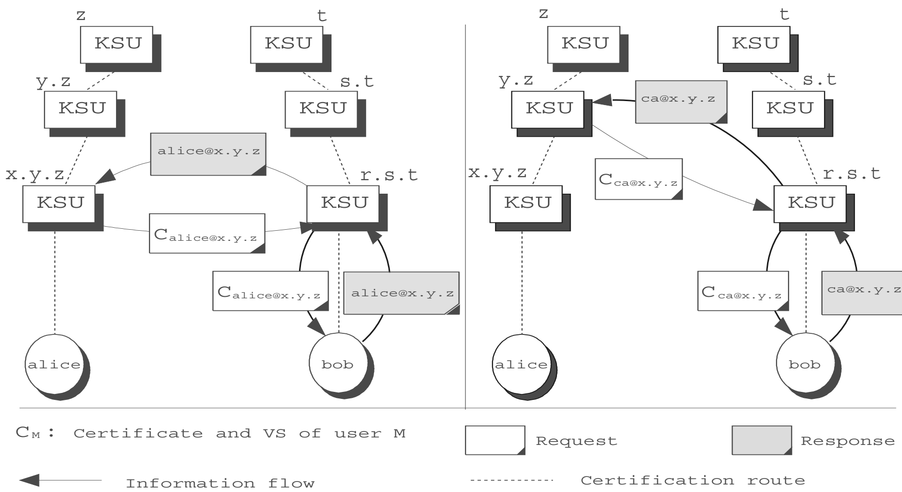
r for , i our sc m , t c rtificat do s ot d to b issu d o -li ; o r, it still pro id s a good d gr of s curit agai st attacks t at tr to us r ok d c rtificat s.

d scrib o t s qu c of actio s t at ar carri d out a us r (r qu st r) a ts to g t t public k of a ot r us r (addr ss). is proc ss starts t -mail addr ss of t last o is pro id d b t r qu st r to is/ r K , a d t is o , i tur , co ducts t r qu st to t addr ss K , os databas co tai s t k . uc op ratio is asil do b caus t s st m ca d t rmi t K to b co tact d from t mail addr ss pro id d.

r ious actio s ar s o d i figur 3 (l ft). I t is cas , t figur d picts t i formatio flo produc d us r *b* (*b b@r.s.*) r qu sts t k of us r *li* (*li* @ . .). s s o , *b* r qu sts lic 's k from is o K a d t is o dir cts t r qu st to t K locat d at t . . od . r spo s from lic 's K is t for ard d to *b*.

b must r qu st t k from is K du to t acc ss r strictio s t at ot r K s s t, a d also to tak ad a tag of t c rtificat cac of is K . If co sid r d, *b* ca also r qu st t c rtificat of @ . . from t K locat d at . , obtai i g a c rtificat t at pro s t aut ticit of t first o . is is d pict d i figur 3 (rig t). asc di g alidatio proc ss ca co ti u u til a top-l l od is r ac d. If o K is pr s t at . (i. . t domai do s ot support rt' s st m), t k of @ . . is automaticall r qu st d from t par t od , t at is, . is allo s rt' to b us d i cas of i compl t structur s.

om similariti s ca b fou d b t rt' a d t *r -* pro-posal [, 2]. ot us t I t r t domai am i rarc to fi d t locatio



e fica e Re e ef a a a gh

r a particular k is stor d, but cur - us s t am r r fil s il rt' us s t -mail offic s. ur c oic is bas d o t follo i g r aso s:

- pposit to -mail offic s, it is usual t at s ral domai s s ar t sam ; t r for , it is fr qu t t at s ot clos l r lat d to us rs, a d t ir s ma ot a dir ct k o l dg of t us rs id titi s, b i g mor ul rabl to imp rso atio .
- s ar i t d d to stor i formatio about domai s, ot about us rs. s a co s qu c , t r is a r gistratio proc dur for a domai but ot for a us r of o of t r gist r d domai s. I fact, t r is o d t at a fi al us r r i t racts it t to g t acc ss to I t r t, but us rs ar forc d to i t ract it -mail offic s to s t up a -mail accou t.
- s us cac i g a d lif tim m c a isms t at could i ld i accurat or fals i formatio i som situatio s. is f atur ca b us d to attack t s st m.

or t s r aso s t cur - sc m ca ot guara t t li k b t r al- orld us rs a d k s (ot co formi g it articl .2 i [3]).

l r s

of t ad a tag s of rt' is t at, i cas t pri at k of a us r is compromis d or lost, t associat d public k ca b r ok d or r plac d it out poss ssi g t pri at o . is is possibl b caus t r is a tit (t), r spo sibl for t mai t a c of t databas of c rtificat s, ic ca p rform a r al- orld us r id tificatio . ppos d to ot r s st ms t at

r quir t at t us r g rat s a “suicidal ot ” to b us d i cas t k is compromis d or lost [4], rt’ us rs do ot d to tak a pr tio m asur s for t is circumsta c .

I cas t k of a is c a g d, isti g c rtificat s must b discard d, a d t must r issu all t c rtificat s. t r s st ms d to otif t is t to us rs a d r qu st old c rtificat s i ord r to r -c rtif t ir k s a d distribut t c rtificat s. I rt’ , a k ps t c rtificat s of its us rs i a local databas of t K , a d t r is o d to s d c rtificat s a d otif t i alidatio of t pr ious o s. o s qu tl , t c a g of t k is tra spar t to us rs.

suall , t d to c ck s for c rtificat r ocatio s b com s a p rforma c a dicap. or t is r aso , s st ms t at us s or similar m c a isms (.g., -li rtificat tatus rotocol [5], or uicidal ur aus [4]) to i alidat c rtificat s i corporat solutio s to mi imi t umb r of acc ss s d d to rif a c rtificat , but t s solutio s ar som tim s artificial a d ot ffici t. r for , a oidi g t us of s as b co sid r d o of t priorit goals i t d sig of rt’ .

I ord r to ac i a d sig t at do s ot pos t probl ms of usi g s il still r tai i g t ir b fits, all t i formatio r lat d to t c rtificatio of a sp cific us r must b locat d a d ma ag d at t corr spo di g K . I cas a d cid s to r cord c rtificat i alidatio ts, a *l In li i n* (I) ca b ma ag d locall . otic t at a I is compl t l diff r t to a b caus t I ill b us d clusi l b t .

a us r c rtificat ds to b i alidat d (b caus is/ r k as b lost or compromis d, or b caus t as r aso s to c as c rtif i g t us r) t simpl d l t s t c rtificat from its databas a d, if appropriat , stor s t r ok d c rtificat i a I . is proc dur is simpl , imm diat , r quir s o commu icatio a d ca pro id proofs of t c rtificat r ocatio s i cas t ds t os proofs.

c t r ocatio tak s plac , isti g acti c rtificat s ar ot us ful a mor b caus o ill b issu d to mak t m alid. us of t pr ts attacks bas d o old c rtificat r us .

. s r I i c i

d sig i g a k ma ag m t s st m t at ac i s s cur us r id tificatio it is c ssar to tak i to accou t t diff r c b t t r al orld (r p opl , compa i s a d comput rs ar), a d t I t r t orld (r am s, k s a d c rtificat s ar).

It must b poi t d out t at ma of t id tit c rtificat s pr s tl us d b ma sc m s ar bas d clusi l i a co tact, t roug I t r t, b t t us r a d t . is is cl arl u satisfactor b caus t r qu st r of a c rtificat ill usuall r quir som guara t of t li k b t t id tit of t us r i t r al orld a d is am i t I t r t orld. r for , i t s c rtificat s, trust is misi t rpr t d from t start.

d sig of rt' guara t s t at a ill o l c rtif t k s of t os us rs clos d to it. r for , a formal id tit rificatio proc dur as b stablis d to gi a l gal m a i g to c rtificatio proc ss [6]. o s - qu tl , a li k is stablis d b t t id tit docum ts (alid i t r al orld), a disti guis d am i t I t r t orld (t -mail addr ss) a d a cr ptograp ic k .

It as b d scrib d o rt' us s t -mail addr ss s to id tif us rs. r ar t o commo criticisms about t us of -mail addr ss s as disti - guis d am s. irstl , it is claim d t at t r latio s ip b t a p rso i t r al orld a d a l ctro ic mail addr ss is ot o -to-o b caus a us r ca a s ral -mail accou ts a d diff r t alias s. sid s, t r ar c r- tai -mail addr ss s t at do ot r pr s t a si gl us r but a group of t m. co dl , it is also claim d t at, i som cas s, t alias fil ca b modifi d it out admi istrator or root p rmissio s. rt' as b d sig d to o r- com t s probl ms b isolati g t c rtificatio ma ag m t from t mail accou t ma ag m t.

4 r r cc ss r c l

I t is s ctio i troduc t protocol t at d scrib s o bot , i di idual us rs a d ot r k s r rs, acc ss a K . co ctio to t port 5 is us d for rt' s r ic . r qu sts ar r pr s t d i a li t/ r r sc a- rio, r i di idual us rs or k s r rs ca pla t cli t rol ; for i sta c , co sid r a r qu st from us r *b b@r.s.* (cli t) to t K locat d at *r.s.* (s r- r), follo d b a r qu st from t K locat d at *r.s.* (o cli t) to t K locat d at . . (s r r). I t subs qu t d scriptio ill b us d to d ot a g ric cli t a d to d ot a g ric s r r.

. r c

ill us t follo i g data structur s as part of t protocol:

li n I : Id tificatio of t cli t.

s rI : -mail addr ss (it format *n* @ *in*) of t us r os k (c rtificat) is r qu st d. rt' us s t *in* to d t r- mi i ic K t k r sid s.

r : .5 9 3 c rtificat co tai i g amo g ot r i formatio : t us r id tificatio (qui al t to *s rI*), t us r's public k , a c rtificat s rial umb r t at is u iqu for t issui g a d t p ct d acti it p riod lif of t c rtificat . is r cord is k pt i t K databas , so t r 's o d to produc it o li .

s : tim stamp stat m t co tai i g a c rtificat s rial umb r, a d t tim of issua c of t is *s* , sig d b t . It is us d to guara t t at t c rtificat it t at s rial umb r as ot r ok d at t tim of issua c . pposit to t *r* t is r cord is produc d o li .

r I : rtificat id tificatio co sisti g o t *s rI* of t addr ss us r a d t c rtificat s rial umb r of t acti c rtificat to b c ck d.

n k : gati ack o l dg m t. It guara t s t at t r is o k associa- t d to t *s rI* r qu st d.

. r c scrip i

protocol is structur d i t r p as s: co ctio , tra sactio a d t rmi- atio .

c i s

co ctio is stablis d it t follo i g m ssag :

: H [cli tI]

r *li n I* is optio al, d p di g o t particular K s curit polic to b impl m t d.

ac ca s t r strictio s to limit t us rs or comput rs allo d to acc ss t s r r. a s r r r c i s t is m ssag , it c cks t r or ot *li n I* is allo d to stablis t co ctio . ft r ards, t s r r s ds o of t follo i g m ssag s as a r spo s :

: + K – t cli t as p rmissio

: - – t cli t ost is ot allo d

: - 2 – t cli t is ot allo d

r s c i s

t co ctio is succ ssfull stablis d t cli t ca start r qu sti g k s. or t is purpos t follo i g m ssag is us d:

: K Y us rI

t s r r r c i s t pr ious m ssag t follo i g situatio s ca aris :

. r qu st d *in* coi cid s it t *in* of (i. . t r qu- st d k b lo gs to a local us r of). r spo s is:

: K Y c rt s

if t k as fou d, or

: - K ack ; – o suc k

if t k as ot fou d.

2. r qu st d *in* do s ot corr spo d it t at of .

a) r qu st d *n* is .

i. If t *in* of corr spo ds to t par t of t r qu st d *in* , t t k s ould r sid i t databas of ; t r for , t cas is ma ag d as a local c rtificat r qu st (cas).

ii. t r is , t k is r qu st d from t K locat d at t upp r od of *in* . If t r is o K i t at od t r qu st is r dir ct d to t succ di g upp r o u til t top-l l od or ar r ac d.

b) r qu st d *n* is ot .
  i. If *in* do s ot ist t s r r r tur s a rror m ssag :
  : - 3
  ii. t r is , a co ctio is stablis d to r qu st t k from t K locat d at *in* . r sult of t is r qu st is for ard d to t r qu st r.

I cas a cli t alr ad as a acti c rtificat t r 's o d to r qu st t compl t c rtificatio i formatio . k c ck m ssag is us d i t is cas .

: HK K Y c rtI

o ic t s r r r spo ds:

: s

if t k is fou d a d as ot b r ok d; ot r is , t r qu st is carri d out as a r qu st.

r i i s

is p as is m a t to i form t s r r t at t cli t as fi is d r qu sti g k s. o do so t cli t s ds t is m ssag :

: I

5 cl s s r r s

ral KIs a b propos d i t lit ratur to m t t s curit ds of diff r t t ork applicatio s. is pap r pr s ts a sc m , rt' , a k ma ag m t a d c rtificatio s st m t at is bas d o t structur of t l- ctro ic mail s r ic a d o t pri cipl of ar-c rtificatio . It pro id s s cur m a s to id tif us rs a d distribut t ir c rtificat s, limi ati g probl ms associat d to commo r ocatio proc dur s, a d simplif i g t alidatio of c rtificat s.

s st m as b d plo d for c rtifi d l ctro ic mail i t i rsit of alaga, a d pr s tl s r ic s about fort t ousa d us rs distribut d i mor t a t t K s. dditio all , t is s st m as r c tl s l ct d b t atio- al s arc a d cad mic t ork i pai to pro id t public k s r ic for its s cur l ctro ic mail s r ic , a d is pr s tl b i g t st d b a r stric- t d group of us rs, as t pr ious st p to its distributio to t commu it of dI I us rs. is is produci g aluabl i formatio for futur impro m ts. mo g t o goi g proj cts, poi t out t utili atio of rt' i cor- porat tra ts, as ll as s ral applicatio s i t i rsit iro m t lik comput r s st m acc ss co trols a d s cur c a g of official docum ts.

f r c s

U De a e f T a e a , g fi e ce E ec c e ce a D c e , a ch
h , The U e f E c e be f e he ca , *d n-s in r t , r din s f Y '* , S ge e ag, 8 , 5 4
h , e a , The e be e he ca Se ce 5 , R 5 ,
http://www.ietf.org/rfc/rfc1510.txt
4 D Da , e be P RS f e eb Sec , *irst rksh n tr ni mm r* , 5, 85 88
5 R a e a , Ya ha g e g e be h P b c e g a h , *n-t rn t i t m si m n t rk nd istri t d st ms rit* , EEE P e , 5, 4
Sch e , D , Sca g he eb f T b g e be a P P P e a ge Sca e he ca , *hni nf r n* , 5
D ffie, e a , e D ec g a h *r ns ti ns n nf rm ti n h r* , T , , 44 54
8 e a a Te ec ca U , Rec e a X 5 *nf rm - ti n hn - n st ms nt r nn ti n - h ir t r th nti ti n r m rk,*
E , SP Re e e , e e af , a
http://www.ietf.org/internet-drafts/draft-ietf-spki-cert-req-03.txt
E , a , a , R R e , Th a , T Y e , SP e fica e The , e e af , e
http://www.ietf.org/internet-drafts/draft-ietf-spki-cert-theory-05.txt
D Ea a e, D a a e S e Sec E e , R 5 5, a ch
http://www.ietf.org/rfc/rfc2535.txt
D Ea a e, , S g e fica e he D a a e S e D S , R 5 8, a ch
http://www.ietf.org/rfc/rfc2538.txt
E ea , P a f a E ea Pa a e a c D ec e a a e f E ec c S g a e , 8 fi a , 8
http://www.ispo.cec.be/eif/policy/com98297.html
4 R R e , a e E a e Re ca , *r din s f th nd n-t rn ti n nf r n n in n i r t r h ,* ' , S ge e ag, 8
5 a , e , a a , R e , S a e , X 5 e e P b c e f a c e e e fica e S a P c SP , e e af ,
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocsp-08.txt
gh , a g be e e a S g g Ta Re h Pe a e fica be , e a c ca , 8

A Method for Developing Public Key Infrastructure Models

Klaus Schmeh

secunet Security Networks AG, Im Teelbruch 116
45219 Essen, Germany
schmeh@secunet.de

Abstract. This paper introduces a method for modelling Public Key Infrastructures (PKIs). This method is referred to as 3PPM Method (Three Part PKI Model Method). The resulting models are referred to as 3PPMs. 3PPMs are based on the Unified Modelling Language (UML). The 3PPM Method can be used in an early stage of PKI setup. It provides for an easy way to obtain a model that can be used as a basis for further planning, training and documentation. The 3PPM method has already been used in practice by the author of this document.

1 Introduction

The conception and the setup of Public Key Infrastructures (PKIs) can be regarded as one of the main issues in the field of computer security today. Before the set up of a PKI starts, it is important to develop a sophisticated model, which visualises the main PKI components and procedures. With a well-designed model it is easier to prepare the PKI setup, to estimate costs and to avoid misunderstandings. The scope of this paper is to introduce a method for modelling PKIs. This technique is referred to as **3PPM** Method (Three Part PKI Model Method), the resulting models are named 3PPMs. 3PPMs are based on the Unified Modelling Language (UML). The 3PPM Method has already been used in practice by the author, who has two years of practical experience in the PKI area.

2 A PKI Set Up Procedure

For the set up of a PKI an appropriate set up procedure has to be found. According to the author's experience the following procedure can be applied:

- Modelling of the PKI: In the first step a PKI model should be developed according to the operators requirements. This model should be based on a requirement analysis and can be used for all future work.
- Product evaluation and basic tests: Before the PKI installation has started, some basic tests can be performed. This is the second step of the set up procedure.
- Pilot: The third step is a pilot, where a small user group works with a test PKI.

- PKI roll-out with one application: When the pilot is completed, the company-wide roll-out of the PKI can start. It is recommended to start with only one application (for example e-mail signatures and encryption).
- Adding applications: When the PKI works with the first application, other applications can be added.

This procedure has many advantages in practice. The experience made in a certain step can be used directly in the next one. Mistakes detected in a step can be avoided in the next one. It is important to note that PKI modelling is the first step in this procedure. It is virtually impossible to understand a PKI or to exchange any thoughts about it without an appropriate model. How such a model can be developed with the 3PPM Method, is described in this paper.

3 Basic PKI Units

The 3PPM Method for PKI modelling uses the terms *component*, *role* and *use case*. These terms are defined in this chapter.

3.1 Components

A **component** is a basic unit of a PKI. A component consists of hardware and/or software, typically it is one computer running a certain software. Typical PKI components are the following:

- Certification Authority: This component is the core part of a PKI. It is responsible for generating and signing certificates.
- Certificate Server: The Certificate Server is a directory server, which provides certificates to the user. The user can connect to the Certificate Server for obtaining certificates or for checking the status of a certificate. For the latter revocation lists can be used.
- Timestamp Server: This component creates timestamps, which are needed to connect a digital signature to the time when it was created. A Timestamp Server is not a compulsory component of a PKI, but it makes a PKI more secure. In many cases, the Timestamp Server is omitted in the beginning.
- Local Registration Authority: This component is responsible for accepting certification requests and for giving them to the Certification Authority.
- Revocation Service: This component is necessary for accepting revocation requests.
- User Components: These are the components used by the PKI user for signing, encrypting and interacting with the central PKI components. Examples for this are E-Mail crypto programs, crypto enabled Web Browsers, hardware crypto components and the like.
- Personal Security Environment (PSE): This component is used by the user to store his private keys. It can be a file on a hard disk or floppy disk, or a smart card.

In any case, a component is a machine. A person is not considered a component.

3.2 Roles

Apart from hard and software, humans play a role in a PKI. A PKI is operated, administered and used by humans. For this reason, roles are defined. A **role** is a set of rights and responsibilties that is connected to one or several persons. One person can have several roles, each role can be carried out by one or more persons.

The roles that have to be determined for a PKI are pretty much dependent on the PKI products used. Typical roles are the following:

- PKI Planner: This is the chief of the whole PKI environment. The PKI Planner commands all other roles, but he is not responsible for administration or routine tasks.
- CA Administrator: This role administers the Certification Authority. A CA Administrator is responsible for certificate generation and certificate revocation.
- Certificate Server Administrator: This role administers the certificate server.
- LRA Administrator: This role is responsible for a Local Registration Authority.
- User: The PKI user is considered a role, too.

Usually there are several people connected to one role (for example if two CA Administrators are needed).

3.3 Use Cases

Apart from persons and machines, processes play an important role in a PKI. For this purpose, use cases are introduced. A **use case** (sometimes also referred to as a business process) is a process that appears repeatedly inside a productive organisation. Usually the following use cases appear in a PKI:

- User Registration: This use case needs to be carried out to register a user for obtaining a certificate.
- Certificate Generation: This use case is carried out to generate a key pair for the user and to create a certificate around it. This use case is necessary after the user has been registered.
- Certificate Revocation: A certificate has to be revoked, when it shall not be used any more. The revocation of a certificate is a use case.
- Certificate Server Inquiry: This use case is carried out, when a user wants to access the Certificate Server to obtain a certificate or certificate status information.
- Timestamp Inquiry: This use case is carried out, when a user needs a timestamp from the Timestamp Service.

Additional use case may be defined for certificate renewal, CA key change, information distribution and other procedures.

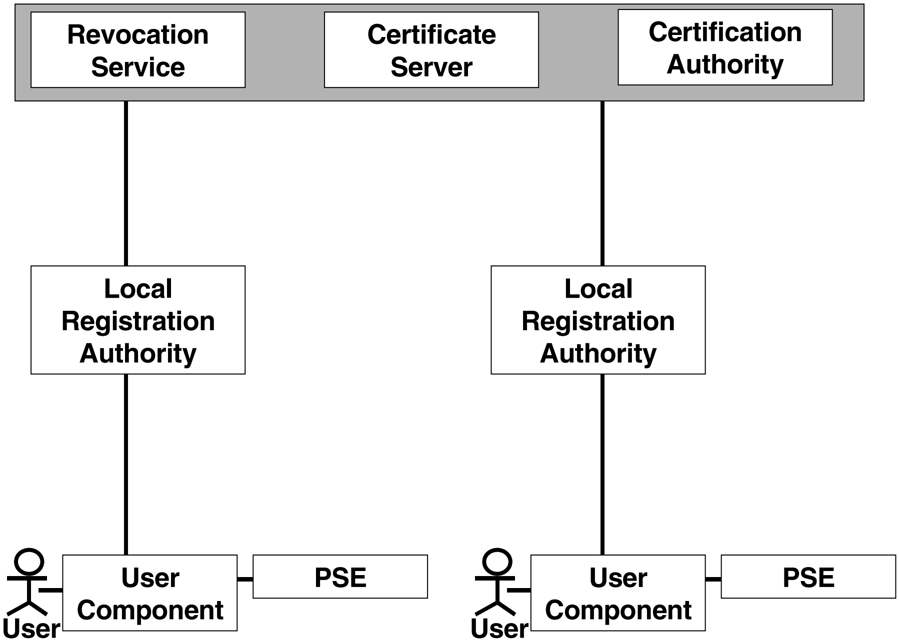


Fig. 1. The components of a typical PKI shown in a component diagram. Central components are the Revocation Service, the Certificate Server and Certification Authority. Each user works with a User Component and a Personal Security Environment (PSE) respectively

4 Identification of Components, Roles and Use Cases

The first step of the 3PPM Method is the determination of components, roles and use cases. There is no algorithm for finding components, rolls or use cases, so it is more a question of experience and creativity. The following subchapters give some guidelines.

4.1 Determining Components

To determine PKI components, it must be decided, which kind of components will be used and how many of each are needed. A Certificate Authority is always necessary, unless certificate generation is outsourced. In a large PKI, several Certificate Servers and Timestamp Servers can be used. It goes without saying that each user should have his own User Component and his own PSE.

Complex PKIs may also include more than one Certification Authorities. For example, hierarchies of Certification Authorities may occur. In this case, there is one Certification Authority issuing certificates for other Certification Authorities, which themselves may certify subordinate Certification Authorities or users. Another option

is a cross certification. In this case there are two Certification Authorities certifying each other respectively. In any case, each Certification Authority is a component.

Local Registration Authorities are another kind of component, which may appear more than once in a PKI. If a high degree of security shall be reached, each user should be required to show up personally at a Registration Authority, which means that at each location of an organisation a Local Registration Authority should be reachable. On the other hand, one central Registration Authority is sufficient, if personal registration is not required. In any case, each Registration Authority is a component.

Of course, it must also be determined, what kind of components are used by the user. This means that the functionality of the user client must be defined. Usually, the user uses tools for mail encryption and file encryption. Special clients for securing WWW connections or SAP R/ 3 transactions are also possible.

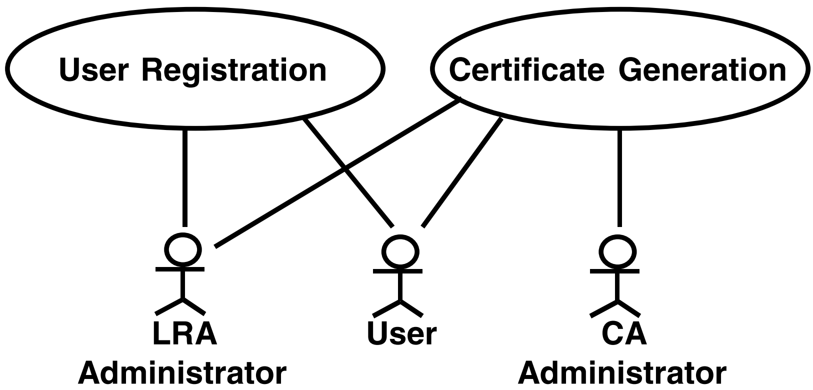


Fig. 2. A Use Case/Role Diagram showing two Use Cases and three Roles

4.2 Determining Roles

It is clear that user roles have to be defined. For the central part of the PKI usually all the roles mentioned in chapter have to be introduced. The whole PKI operation and PKI construction should be managed by a Site Planner. For a Certification Authority and for a Certificate Server administration roles have to be defined. Of course, administration roles must be adjusted to the software used, but all major PKI software systems support administration roles. The user role must also be determined: It must be clear, which members of an organisation may act as users and which other persons (e.g. customers) are accepted.

Additionally, it must be determined, how many people carry out a role. Privileged roles should always be carried out by more than one person in order to make sure that there is always a person with privileged permissions available.

4.3 Determining Use Cases

The use cases appearing in a PKI are usually always the same (see chaper), so it is not difficult to identify them. The more critical part is to determine how exactly they look like. This is pretty much dependent on the security policy and on the IT infrastructure of the organisation setting up the PKI.

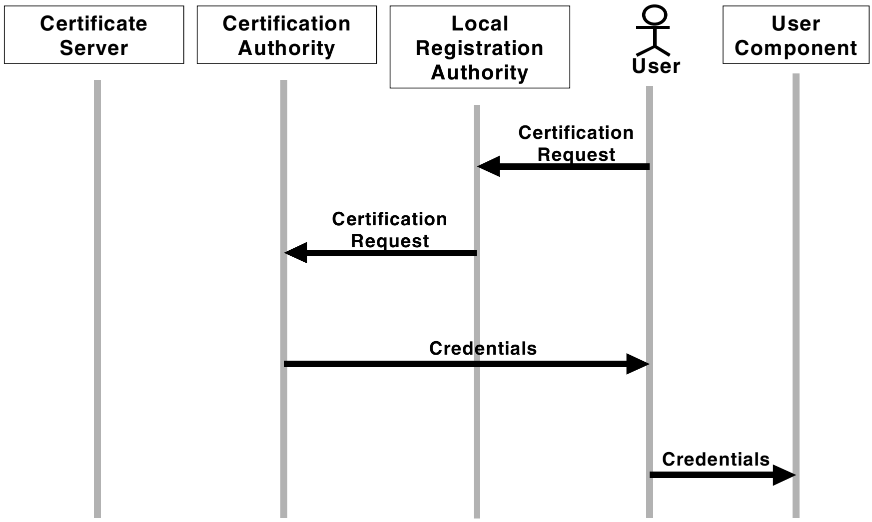


Fig. 3. A PKI Use Case modelled with a sequence diagram

A crucial part of a PKI set up is the determination of the use case Registration and Key Generation. It must be clear, whether a user must show up personally at a Registration Authority to register for a certificate or if an e-mail registration is sufficient. It is also important to know, whether users generate their keys themselves or whether a centralised key generation is applied.

5 Developing A Three Part PKI Model

The second step of the 3PPM Method is the development of the model itself. The model consists of three parts, each part is identified with a certain kind of diagram. Which diagrams are used is described in the following subchapters.

5.1 Component Diagram

The first part of the model is a **component diagram**. A component diagram contains all the components of a PKI. For a better understanding, some of the roles can be

included, too. The units interacting with each other are connected with a line. Figure shows an example for a component diagram.

5.2 Use Case/Role Diagram

The second part of a 3PPM is a Use Case/Role Diagram. In this diagram every use case is modelled with an ellipse, every roll is modelled with a symbol for a person. Figure shows an example for a Use Case/Roll Diagram. Each role is connected to the use cases in which it is involved.

5.3 Sequence Diagram

The third part of a 3PPM is a Sequence Diagram. A sequence diagram lists components and roles in a table, communication actions are modelled with arrows. An example for a sequence diagram is shown in figure.

Sequence diagrams should be used to model the more complicated use cases. To get a sequence diagram for a use case, all communication actions must be found, they are modelled with arrows. On each arrow a description of the data transported is written. If an action takes place with only one component or role involved, the arrow points to the place where it starts.

Not all use cases have to be modelled with a sequence diagram. For the less complicated use cases a text description is usually sufficient. According to the author's experience, the use cases for user registration and certificate generation should be modelled with a sequence diagram. For all others this is not necessary.

6 Benefits of the 3PPM Method

The 3PPM Method enables the development of PKI models, which are easy to understand, even for people not knowing this technique. On the other hand, this method is powerful enough to get a model that covers all of the main PKI issues.

The 3PPM Method has already been used in practice. The author has used in several PKI projects to develop a model for a company planning a PKI set up. Such a model can be used to discuss PKI details and it is a part of the specification. Most of all, a sophisticated but simple model enables the detection of problems and mistakes in an early stage of the set up project.

7 Summary

This paper has introduced a method for modelling Public Key Infrastructures. This method, referred to as 3PPM Method, is based on the Unified Modelling Language (UML). To understand this method, the concept of components, roles and use cases has to be understood. The method consists of two steps: In the first step, components, roles and use cases are determined. In the second step, the model itself is developed.

The benefit of this method is that all major aspects of a PKI can be modelled with it. It is easy to develop a 3PPM and it can be used easily in all later stages of the PKI set up.

References

1. Schmeh, K.: Safer Net – Kryptografie im Internet und Intranet. dpunkt.Verlag Heidelberg (1998)
2. Schneier, B.: Applied Cryptography. John Wiley (1995)

The Realities of PKI Inter-operability

John Hughes

Claridge House
29 Barnes High Street
London, SW13 9LW
England
John.hughes@entegrity.com

Many vendors are claiming that their products are "open" and "inter-operable". This paper is intended to explore what this could mean, and in reality what is available in the market place, highlighting any issues found by the author.

1 Introduction

Public Key Infrastructure (PKI) offers a method of protecting an enterprise's electronic communications using public key cryptography. Because PKI is an "infrastructure", it is usually necessary to obtain board-level approval for funding or to find some sponsor in the enterprise. As this is sometime difficult to justify local business units are implementing secure solutions, that just happen to be PKI based. As a result of this situation PKI Islands are developing.

PKI Islands have the advantage of allowing an enterprise to seed PKI throughout its business without the need to undergo the turmoil of a "big bang" – an approach sometimes termed "PKI by Stealth". However, at some stage an enterprise will need to connect the Islands together and also secure its communications with trading partners. If inter-operability issues have been ignored at the design stage, problems will almost certainly emerge later.

This paper summarises some of the technical issues of making various PKI components inter-operate (or why they cannot operate with each other!). Entegrity Solutions have defined an ***Inter-operability Model*** which is used within the company to examine areas of product deficiency and product enhancements providing additional flexibility.

2 Inter-operability Model

Whist the PKIX have defined a Certificate and CRL profile, one has not been produced for all elements of a PKI. The intent of the Model is to assist in formulating such profiles. Following a summary of the model the paper summaries some of our experiences in achieving interoperability.

The major elements that the Interoperability Model covers are summarized in the following paragraphs.

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 127–132, 1999.

- Key Generation. Three basic key generation schemes are possible: Centralized at the CA, at the EE Client or to have Split Keys. In this last case one set of keys are generated at the EE for a particular set of purposes and another set generated at the CA.
- Encapsulation protocol. *If the public key is generated at the EE then a means of securely sending the public key and receiving back the certificate is required. Four main encapsulation protocols are (or will be soon) available from products. These protocols are PKCS#10-PKCS#7, Verisign's CRS, PKIX CMP and PKIX CMC..*
- Transport. *The encapsulation protocols provide message protection. However they still have to be transported around the network. Whilst web-based http is clearly the natural (and dominant) technique, it is actually quite complicated partly due to the authentication issue (see below). As those with Internet issued certificates will be aware, obtaining them for a Web Browser is a painful multi-step process, involving a number of Web dialogues plus an e-mail transaction. Because it is a manual, user driven process, most Web Browsers can interact quite successfully with CAs. However dealing with other applications illustrates the point that in general PKI-enabled applications are not well integrated with CAs.*
- Authentication. There are two basic schemes involved in authenticating the owner of a public key prior to its certification. In the case of class 1 VeriSign certificates, no real authentication is actually performed. Therefore anyone could claim a false identity and obtain a certificate issued in that name. This is not the case though for higher grade certificates, such as VeriSign class 3 certificates. The authentication schemes generally available are:

  – Manual approval at the CA
  – Automated approval at the CA using some type of "secret value" look-up
  – Centralized Token issuing with pre-authorization information.

- Token/PSE Format. There is no widely deployed standard that currently defines the format and contents of the PSE. Currently a new standard is being drafted with the intention of defining the PSE for Smart Cards – this is PKCS#15.
- Token Plug and Play. When using physical cryptographic tokens the emerging dominant API standard is PKCS#11. Most smart card vendors and high-end cryptographic accelerators support PKCS#11. PKCS#11 defines an API to add, modify and use cryptographic keys on the Token. The intention being for a PKI application supporting PKCS#11 to plug in any PKCS#11 Token. In reality it's not quite that simple.
- Publication/Retrieval protocol. The market leader in this area is the LDAP protocol. The version of LDAP most widely used at present is version 2 (LDAPv2), but increasingly LDAPv3 server products are appearing.
- Publication Protection. Certificates and CRLs are self-protecting objects, and therefore the connection for publishing them on the LDAP server, at first sight, does not seem to require protection. However as the connection requires "write access" to the server, it is important to control access to limit those network entities that can write to the server. The techniques used to protect this connection, include SSL.

- Schema. Publishing the PKI Information on the LDAP Server requires the server to be configured with defined X.500 attributes and object classes. X.500 defines the required attributes, such as userCertificate. However the object classes, as originally defined, are not suitable for PKI deployment. PKIX has defined new Schema object classes that solve the original problems.
- OCSP. CRLs are not the only mechanism available to determine whether a certificate is still valid and has not been revoked. A new standard and technology called On-line Certificate Status Protocol (OCSP) is being developed. Another technology called Certificate Revocation Trees (CRT), offered by Valicert, is yet another certificate revocation mechanisms. All 3 mechanism have different characteristics, and each one has its benefits and problems.
- *Certificate.* A Certificate is a very complicated structure and can contain many optional fields. A X.509 v3 certificate can have, none, one or more extensions fields. A number of standard extensions are defined by ISO/IETF – but it is also possible for various industry groupings to define their own extensions. Given the complexity and richness of the Certificate together with its various optional fields, inter-operability manifests itself as a problem. Therefore one aspect of the PKIX working group has been to develop a certificate profile to increase the probability of inter-operability of systems using PKIX conformant certificates. This is defined in RFC2459.
- CRL *RFC2459 also contains a profile for CRLs based on the ITU-T X.509 CRL version 2 standard.*
- *Cross-certification* In some topologies there is a requirement for peer CAs to certify each other's public keys and then publish them in the form of cross-certificates. Cross-certification can take be performed either manually or automatically.

3 Our Experiences of Interoperability

Entegrity Solutions are focused on delivering Secure Applications based on the *Entegrity Secured Application Platform*™ working within many different CA vendor environments, our CA Partners include CyberTrust, VeriSign and IBM. Our intent is to be inter-operable in as many PKI environments as possible, both the infrastructure and the PKI-enabled applications. This paper concentrates on our experiences of interoperability testing with many different CA vendors, but also touches upon other areas.

3.1 Certificate and Certificate Path processing

In general all Certificates from the main CA vendors seem to be well constructed and can be decoded. However note that there are some aspects that could rise to inter-operability issues:

- Some Cas do not have the ability to support RFC-822 names in the X.509v3 alternate name extension. What is quite common is to use the "EA= " attribute in

the DN rather than a RFC-822 Alt Name. This can give rise to problems to some secure e-mail packages expecting the Alternative Name extension (or vice versa)

- Some times you do see non-standard OID encoding in the DN (e.g. OID.2.5.4.5=123). This technique is also sometimes used to carry RFCS-822 names in the DN
- Obviously private extensions in a X.509v3 certificates can give rise to problems, especially if they are marked critical (which fortunately is rare). The biggest culprit in this area is Microsoft.
- The Key Usage, Basic Constraints and Subject KeyID extensions are now widely used, although some older products do not support these features.
- There seems to be wide variety concerning the Authority KeyID extension. It is either not used, or either the hash or issuer name method is used. It's not clear whether all EE PKI-Enabled s/w can cope this variety.

We have found that using our technology Certificate chain validation is not a problem. All CA vendor products we have tested successfully pass our tests.

3.2 ASN.1 Encoding problems

Given that ASN.1 is such a rich standard with various encoding rules, but yet its frequently specified partially in English, its not surprising that ambiguities or implementation problems manifest themselves. Surprisingly they do not appear in encoding X.509 certificates. Recently we have discovered two problems with products in other areas.

- If you send a S/MIME-PKCS#7 message to a well known web browser/e-mail client that has a mixed BER/DER encoding it crashes (although earlier versions handled it OK)
- If a PKCS#10 certificate request is sent to a well know CA product that has any BER encoding then it can not parse the request

This illustrates the point that not all PKI based products, whether Infrastructure components or PKI-enabled applications, can cope with the vagaries of a full ASN.1 implementation. Some products only expect DER encoding.

3.3 LDAP

In theory LDAPv3 is a superset of LDAPv2 and hence any LDAPv2 client (for instance a secure e-mail client) should be able to retrieve certificates and CRLS from a LDAPv3 server. In reality this is not true. Fetching certificates/CRLs means that they need to be transferred as binary objects. LDAPv3 states that the LDAP client, when requesting a binary object, needs to specify the ";binary" key word with the name of the attribute being fetched.

Publishing to a LDAP server is also problematic, although in the main it is an easy problem to resolve. The original definition of the PKI attributes, such as userCertificate meant that the user's LDAP entry and this attribute be created in one atomic operation. To get around this problem CA vendors defined new object classes

that permitted all CA information being written to the LDAP server was optional. Until recently all products had their own definitions and names for these object classes, although in general they were very similar. Recently PKIX has standardized on 2 new object classes pkiUser and pkiCA. This approach demands that the LDAP server can be configured with these new object classes.

3.4 Certification Requests

The prevalent certification model deployed is that of using a communication of Web and e-mail. The steps one would take being similar to the following:

- User would browse to the CA's web page
- An option on the page would be to generate a key pair and request a certificate. Prior to this the user will be prompted to enter personal information used for both identity authentication and creation of the certificate.
- Selection of this option would cause a http message to be sent to the browser that triggers a key pair to be generated and the public key sent back to the CA (usually in the form of a PKCS#10 request). The browser being triggered to perform these functions by specific mime types in the http message.
- The CA would respond with a message saying that the certification request is being processed and that e-mail will be sent on how to pick up the certificate. Typically a request number and password will be provided (or defined by the user).
- When the certificate has been generated, instigated either via a manual or automatic approval process e-mail is sent to the user.
- The user then goes to the "pick up certificate" web page and requests the certificate, entering authentication information as appropriate. A http message is sent to the browser and because the http message has a particular mime type it causes the browser to "swallow" the certificate and place it in the appropriate certificate store

On-line certification outside a browser environment is not as well specified. Whilst most CA products permit this approach all the CA products have different methods to achieve it. Different MIME types are used by the CA products and various techniques for parameter passing.

3.5 PKCS#11

Whilst PKCS#11 was created a number of years ago it is only recently that Smart Card and High Security Module (HSM) suppliers have started to release PKCS#11 based device drivers. Because there is no recognised conformance test suite, in our experience, the quality of the implementations in general are not that good.

3.6 PKCS#12

PKCS#12 is a useful mechanism to transfer information between different PKI components - e.g. from transferring EE information from a RA/CA into the EE's PSE.

However not all RA/CA products can create PKCS#12 files containing the full certificate path. That is they can only populate it with a key pair and the user certificate. If a RA/CA has this limitation then it not possible to create a EE PSE in a single step as the trusted certificate, and any other subordinate CA certificates would have to be loaded via other means.

4 Conclusions

Certificate and Certificate Path processing becoming are becoming “trivial” and there is wide spread inter-operability between PKI products.

However there are some immediate problem areas that need to be addressed:

- Tighter CA and EE integration and standardisation, in particular in the area of on-line certification not using browsers
- More robust and compliant PKCS#11 implementations
- Standardized PSE/Token formats (soft and hard)

An area that more work is required on is that of the new generation of PKIX CMP and CMC management protocols. To date there are very few products that support these, therefore limited interoperability work has been accomplished. What interoperability problems there are will become evident by the beginning of next year as products supporting these protocols are released into the market.

Mobile Security – An Overview of GSM, SAT and WAP

Malte Borcherding

BROKAT Infosystems AG, Industriestr. 3,
D-70565 Stuttgart, Germany
Malte.Borcherding@brokat.com

Abstract. Mobile networks have become a very attractive channel for the provision of electronic services, as they are available almost anytime and anywhere. But for a service provider, there are several mobile communication standards to choose from. They differ in market penetration, flexibility, and security.

This paper gives a comparative overview of the security features of GSM, SIM Application Toolkit and WAP (Wireless Application Protocol). It describes the trust relations involved, and gives examples of typical applications suitable for each of these standards.

Results are that pure GSM is suitable only for applications with low sensitivity, as the security features are limited. SIM Toolkit allows for the implementation of application-specific end-to-end security, and is thus suitable for sensitive, personalized applications like banking ore brokerage. Finally, WAP defines a security standard with choices for differently strong algorithms. In order to be suitable for secure applications, the models for local storage have to be settled, and there must be sufficiently many WAP phones with support for strong security on the market.

1 Introduction

Mobile networks have become a very attractive channel for the provision of electronic services: They are available almost anytime, anywhere, and user acceptance of mobile devices is high. As a result, there is a strongly increasing amount of services offered through mobile networks. They range from simple information services to sensitive applications like banking or electronic commerce.

As a related development, standards for mobile applications are maturing, and new standards are being defined. This leads to a set of possible technologies a service provider can choose from. They differ in depth of standardization, market penetration, flexibility and security.

This paper focuses on the security features of GSM, SIM Application Toolkit and WAP (Wireless Application Protocol). It compares the security-related properties and the trust relations involved, and gives examples of typical applications suitable for each of the standards.

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 133–141, 1999.

2 GSM

GSM ("Global System for Mobile Communications" or "Groupe Spéciale Mobile") is a standard for digital mobile telephony, defined by the European Telecommunications Standards Institute (ETSI). The first GSM services were started around 1992. Today, this standard is used globally in more than 300 networks operating in more than 100 countries.

A basic design requirement of GSM was security of communication. The following paragraphs describe the security mechanisms employed, the implicit trust relations, and the suitable types of application for the given security features.

2.1 Security Features

GSM offers confidentiality, subscriber authentication, and subscriber identity confidentiality [2, 5]. The security mechanisms are only defined for the air interface, i.e., security of transport through fixed networks behind the base stations is left to the network providers. The security mechanisms are applied to all traffic, including short messages.

Key Infrastructure: GSM Security is based on subscriber-individual symmetric keys shared between the home network and each SIM card (subscriber identity module). More precisely, there is one key k_i of 128 bit length per IMSI (International Mobile Subscriber Identity). The SIMs are initialized with the k_is during personalization. The individual subscriber keys are usually not transmitted over the network, but used in a challenge-response protocol for authentication and key agreement.

Authentication: In an initial phase of a communication, the network sends a random challenge *RAND* of 128 bit length to the end device. The device computes a 32 bit response $SRES = A3(k_i, RAND)$, where *A3* is an authentication algorithm implemented in the SIM and the network. *SRES* is sent back, and the network compares the received *SRES* with the expected value

Encryption: The symmetric encryption key k_c is derived using the same parameters k_i and *RAND* which have been used for authentication: $k_c = A8(k_i, RAND)$, where *A8* is again implemented in the SIM and the network. The actual data encryption is done using the stream cipher *A5*, which is implemented in the end device (not the SIM) and the network. The maximum effective length of k_c is 64 bit.

Subscriber Identity Confidentiality: The objective of subscriber identity confidentiality is to conceal the IMSI during normal operation by the use of temporary IDs (TMSI), such that an attacker cannot easily figure out who is participating in a connection.

As described above, the algorithms for authentication and key generation (*A3* and *A8*) are implemented in the SIMs and the home networks. If the user is outside the home network, the visited network can request sets of corresponding triples (*RAND*, *SRES*, k_c) from the home network. This allows the visited network to communicate with the handset without gaining access to *A3* and *A8*.

As the SIMs and their contents (including *A3* and *A8*) are controlled by the respective networks, this structure leaves room for national and business policy enforcement. *A5*, on the other hand, has to be supported by all networks and end devices in order to interoperate properly.

Although the algorithms are not published officially, one widely employed implementation of *A3/A8* called *COMP128* and a compatible algorithm to *A5* have been published [9, 12]. *COMP128* has been shown to leak k_i, and attacks against an algorithm similar to *A5* have been published in [10]. Further publications on *A5* are expected in the near future. This has lead to some uncertainty with regard to the actual strength of encryption and authentication of productive GSM networks.

2.2 Trust Relations

Users and service providers relying on the GSM security have to trust the network providers in the following aspects:

- They have to trust all network providers involved in the communication, regarding privacy of information and keying material, and
- the home network provider, regarding proper choice of algorithms *A3/A8*.

2.3 Area of Application

Given the security infrastructure described above, "pure" GSM should only be used for applications with low sensitivity, like public information services. Examples for such services include:

- General information (e.g., weather forecasts, sports results)
- Cell broadcast (e.g., nearest restaurant)
- Non-sensitive personalized financial information (e.g., stock information according to a customer's profile)

Sensitive applications like account statements or financial transactions should employ additional security mechanisms, as described in the following sections.

3 SIM Application Toolkit

The SIM Application Toolkit is a GSM specification which defines an interface between GSM handsets and subscriber identity modules (SIMs) [8]. As described in the previous section, SIMs are smart cards which carry information related to the subscriber and the GSM provider, like individual secret keys, algorithms for key generation and authentication, and the subscriber's address book.

The SIM Application Toolkit allows applications stored on the SIM to communicate through the handset with the user and the network. In other words, applications on

the SIM can use the handset as I/O device with the help of the SIM Application Toolkit. For example, applications can define simple menu structures which set up calls to service numbers, but they can also be used to add security data communication via GSM. More specifically, the SIM Application Toolkit [8] includes the following functionality:

- Display text and menus
- Receive input from the keypad
- Send and receive short messages
- Set up calls
- Communicate with a secondary smart card (for dual-slot handsets)

Although a SIM Toolkit application can be any kind of application running on a given SIM, there are standardization efforts underway within ETSI to define an application programming interface for higher-level languages (SIM API). The goal is to have a framework where a SIM application can access SIM Toolkit features through a standardized API for each relevant programming language. The general framework is specified in [3], and specific Java bindings are given in [4]. A similar specification for Virtual Basic is under consideration.

Apart from defining an interface to SIM Toolkit, the SIM API also comprises functions for access to GSM files on the SIM and low-level functionality, such that an applet can act as the basic GSM application towards the handset.

These standardization efforts lead to a simplified development of SIM Toolkit Applications. A Java programmer can use the standardized interfaces to develop an applet for a Java SIM card which interacts with the external world through SIM Application Toolkit, without dependencies of the specific platform.

3.4 Security Features

SIM applications have access to incoming short messages, and can send short messages by themselves. Hence, they can be used to add encryption and authentication to short messages. There are no limitations to the security mechanisms employed, except those imposed by the technical limits of the SIM.

In contrast to basic GSM security, SIM Application Toolkit allows for an end-to-end-security between the subscriber and a service (content) provider, such that messages can be encrypted, for example, between a SIM and a banking server. This makes security independent of limitations of the GSM algorithms.

There are SIMs capable of RSA computations available, such that RSA-based public-key systems can be used directly on the SIM. Alternatively, implementations of elliptic curve cryptography can be used. But since most GSM providers currently do not use cards suitable for public key systems, most of today's applications are secured by symmetric algorithms.

Short message formats including security features are defined in [6]. The specification covers encryption, authentication, redundancy checks, counter management, and

proof of reception handling. For this purpose, it defines a header to be included in protected short messages. Currently, identifiers for DES and triple DES (two or three keys) are specified for encryption as well as for message authentication.

In addition, there are identifiers defined for proprietary algorithms and for algorithms known implicitly by sender and receiver. This allows for the application of arbitrary algorithms. For key agreement, there are four bits to indicate one of several keys (separately for encryption and message authentication). The actual keys have to be agreed upon through a channel outside the scope of the specification.

There are different possibilities for key distribution, which can also be combined:

- Hardcoded keys which are stored on the card during personalization
- Distribution of keys over the air, using a transport key for security
- User input of key material (complete keys or seed)

The selection of an appropriate scheme depends on the required flexibility of the application and on the security requirements. For example, distribution over the air is useful for key rollover, and user input of key material can be used to establish a shared secret between the SIM and the application server, thus taking the network provider out of the loop.

If a dual-slot handset is used, the SIM Toolkit Application can make use of a secondary cryptographic smart card. This is a useful feature if, for example, users already have a standardized signature card. The SIM application can then coordinate the display of data to be signed, PIN input and the actual signature generation on the secondary card.

3.5 Trust Relations

Although SIM Application Toolkit allows for an end-to-end security, the GSM provider is still involved in the trust relations because it usually owns the SIM. All data put on the SIM, including applications and keys, is in principal under the control of the network provider.

This control can be tight, where the network provider actually puts applications and secret keys on the card, or loose, where the provider gives download keys to the service provider.

The communication parties have to trust the network provider and the card manufacturer in that they do not misuse or leak the (potential) knowledge of information stored on the SIM. A lower level of trust is necessary when the application allows for entering additional keying material shared between the end-user and the service provider. In any case, there is no trust necessary concerning intermediate networks, as is the case for pure GSM security.

3.6 Area of Application

SIM Application Toolkit is most suitable for sensitive, personalized services, such as banking and brokerage. Security mechanisms can be agreed upon individually per application, and the SIM is a very suitable storage device for secret application keys.

One basic application useful as building block for many solutions is a signature application. In such an application, the SIM contains a private signing key and some application logic which controls the signature process. It receives short messages which contain the document to be signed, displays the content to the user, and generates a signature on user demand. The signatures can then be sent back to the source of the document, or to a different recipient. This way, the handset becomes a general-purpose and highly secure signature device. The signature process can be triggered by any kind of external application, like a Web application or a brokerage system driven by stock trading events.

4 Wireless Application Protocol (WAP)

WAP [13] is a protocol stack for mobile environments which enables services similar to the Internet, in particular the WWW. The stack is based on a bearer like SMS messaging or GPRS (General Packet Radio Service). Further layers include transport, security, session and application layers. The application layer defines a markup language called WML which is interpreted in a browser on the client side.

WAP is being defined by the WAP Forum, an industry group comprising handset manufacturers, wireless service providers, infrastructure providers, and software developers. The WAP specification was released in its first version in April 1998. Since then most cellular vendors have been active to develop network components and terminals for WAP. The first services were shown in early 1999.

4.7 Security Features

The security layer protocol in the WAP architecture is called Wireless Transport Layer Security, WTLS [15]. The primary goal of the WTLS layer is to provide privacy, data integrity and authentication between two communicating applications. WTLS provides functionality similar to TLS 1.0 [1], but it is optimized for low-bandwidth bearer networks with relatively high latency. Differences to TLS include specifications for elliptic curve cryptography, small-sized digital certificates, optimized handshake and dynamic key refreshing.

Like TLS, WTLS defines a set of cipher suites, including weak and strong ones. The cipher suite for a connection is agreed upon during an initial handshake phase. Key exchange ciphers include RSA, Diffie-Hellmann, and EC-Diffie-Hellmann, all with different key lengths and partly without authentication. It is also possible to start from a shared secret (established on a different channel), such that no public key cryptography needs to be used. For bulk encryption, the algorithms RC5, DES, triple

DES and IDEA are defined, each with different effective key lengths in order to cover export control requirements. For symmetric message authentication, WTLS specifies keyed MACs based on SHA-1(160 bit key) and MD5 (128 bit key).

For the storage and usage of key material and related personal information, WAP defines a WIM (WAP Identity Module) [14]. A WIM can be in principle any kind of module, but the standard notes explicitly the possibilities to include a WIM application in the SIM or to use an external smart card.

The functionality of the WIM is to support the WTLS protocol, but also to provide application level functionality. For WTLS, it can perform such functions as generation of random numbers, storage and usage of private and public keys, and computation of the various symmetric keys. Functionality offered to applications includes unwrapping of symmetric keys with the help of a securely stored private key, and signing of hashes. These operations can be called from WAP applications through WMLScript (a scripting language similar to JavaScript), or by applications external to WAP.

Security-related data is stored according to PKCS#15 [11]. This allows non-WAP applications to have a standardized access to the keys. It is thus conceivable that a user uses the same smart card for authentication in WAP with WTLS, and in the Internet using SSL or TLS.

4.8 Trust Relations

The trust relations in WAP depend on the position of the WAP server in the network architecture: It can either be hosted by the network provider or directly by the application service provider. In the first case, all parties have to trust the network provider, as the WAP server is one endpoint of the security relation. In the second case, information is transmitted securely between the user and the service provider, such that the network provider has no access to the data.

In contrast to SAT, the network provider has only limited or no control of the applications the user is accessing. This shifts additional responsibility onto the users: They have to assure themselves that the application they use really is what they intend to use. As a prerequisite, it is necessary that CA certificates stored in the end device or the WIM for server authentication are correct and trustworthy.

When a SIM is to be used as WIM, the different trust models of SAT and WAP start to interfere. In SAT, the SIM is used by applications which are known and trusted by the card issuer, while in WAP, the applications are trusted by the user (and not necessarily by the card issuer). By the time of writing, the exact models as to which extent SIMs are opened up to WAP applications are not completely sorted out.

Table 1. Comparison of security algorithms and key lengths

	Secured relation	Bulk encryption	Effective key length (bit)	Authentication[1]	Effective key length (bit)
GSM [2]	Handset to base station	A5 (A8 for key gen.)	max. 64	A3 (client auth only)	128
SAT [6]	SIM to server	DES 3DES any	56 112, 168 any	DES 3DES any	56 112, 168 any
WAP [15]	Handset to server	RC5 DES 3DES IDEA	40, 56, 128 40, 56 168 40, 56, 128	RSA ECDHDSA SHA-1 MD5	512, 768, any any 160 128

4.9 Area of Application

WAP is currently suited best for non-personalized information services which do no require strong client authentication, as models for local storage of key material and other personalized information are not yet completely settled. If there are end-devices with support for strong security in the market, sensitive data can be transported via WAP.

It has to be noted that secure WAP applications require a more security-aware and educated user than in the case of SIM toolkit, as there is no pre-evaluation of applications by the network provider, and the users have to verify the authenticity of the servers by themselves.

5 Summary

For applications over GSM-based mobile networks, there are currently three implementation alternatives: Using standard GSM mechanisms, implementing an application on the SIM using the SIM Application Toolkit, or using the Wireless Application Protocol (WAP). There is no single best choice among the services: Pure GSM offers only limited security, but has the least restrictions concerning capabilities of the handsets. SIM Toolkit allows for the implementation of application-specific end-to-end security, but it is restricted to handsets capable of SIM Toolkit. Furthermore, SIM applications can be used only by those subscribers who have got suitable SIMs from their GSM providers.

---

[1] For WAP WTLS, authentication is achieved through a combination of the asymmetric algorithms and keyed hashes. The mechanisms for anonymous key exchange are not mentioned in this table.

Finally, WAP defines a security standard with choices for differently strong algorithms. Compared to SIM toolkit, it is much more standardized on the application and transport security level, such that any WAP browser can basically connect to any WAP server (provided they can agree on a common cipher suite). In order to be suitable for secure applications, the models for local storage of key material have to be settled upon, and there must be sufficiently many WAP phones with support for strong security on the market.

Table 1 gives an overview of the algorithms and key lengths specified for the three standards under consideration.

References

1. T. Dierks et al: The TLS Protocol, RFC 2246, January 1999, ftp://ftp.isi.edu/in-notes/rfc2246.txt
2. ETSI: GSM 02.09: "Security-related Network Functions", February 1992, http://www.etsi.org
3. ETSI: GSM 02.19: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); Service Description; Stage 1", to appear
4. ETSI: GSM 03.19: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2", to appear
5. ETSI: GSM 03.20: "Security Aspects", June 1993, http://www.etsi.org
6. ETSI: GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit", http://www.etsi.org
7. ETSI: GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface", http://www.etsi.org
8. ETSI: GSM 11.14: "Digital cellular telecommunication system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface", http://www.etsi.org
9. ISAAC Reserach Group at the University of California, Berkeley: http://www.isaac.cs.berkeley.edu/isaac/gsm.html
10. Jovan Dj. Golic: Cryptanalysis of alleged A5 stream cipher, Proceedings of EUROCRYPT '97, LNCS 1233, Springer-Verlag, 1997
11. RSA Laboratories: "PKCS #15: Cryptographic Token Information Standard", Version 1.0, April 1999, ftp://ftp.rsa.com/pub/pkcs/pkcs-15/pkcs15v1.doc
12. GSM Papges at Smart Card Developers Association: http://www.scard.org/gsm/body.html
13. WAP Forum: WAP Architecture Specification, April 30, 1998, http://www.wapforum.org/
14. WAP Forum: Identity Module Specification, Proposed Version July 5, 1999, http://www.wapforum.org/
15. WAP Forum: Wireless Transport Layer Security Protocol, April 30, 1998, http://www.wapforum.org/

Secure Transport of Authentication Data in Third Generation Mobile Phone Networks

Stefan Pütz[1], Roland Schmitz[2], and Benno Tietz[3]

[1] T-Mobil (DeTeMobil, Deutsche Telekom MobilNet GmbH)
PO Box 30 04 63, D-53184 Bonn, Germany
stefan.puetz@t-mobil.de

[2] T-Nova Innovationsgesellschaft mbH
Deutsche Telekom
D-64307 Darmstadt, Germany
Schmitz@tzd.telekom.de

[3] Mannesmann Mobilfunk GmbH
Am Seestern 1, D-40547 Düsseldorf, Germany
Benno.Tietz@d2privat.de

Abstract. In this paper a mechanism for securing sensitive MAP messages between network elements belonging to different network operators is described. The mechanism is currently under discussion in the security group of the Third Generation Partnership Project, a joint project of ETSI and Japanese, American, Korean and Chinese standardisation bodies working on the security specifications for UMTS. The proposed mechanism provides confidentiality, authenticity and integrity of the messages exchanged; however, there may be messages where no confidentiality or no protection at all is needed. Therefore, three levels of protection have been defined that are applied to the various MAP messages according to their sensitivity.

1. Introduction

The security of the global Signaling System No. 7 (SS7) network as a transport system for sensitive signaling messages between different telecommunication network elements is open to major compromise. Messages can be eavesdropped, altered, injected or deleted in an uncontrolled manner. For example, in mobile phone networks based on the GSM (Global System for Mobile Communication) standard, particularly sensitive authentication data of mobile subscribers have to be transported from the Authentication Centre (AuC) to the Visitor Location Register (VLR)[1] in order to authenticate the subscriber.

For the first phases of the third generation mobile system UMTS (Universal Mobile Telecommunications System), a similar approach is foreseen. Transportation of the data will be done via the MAP (Mobile Application Part) protocol [3], a mobile-phone specific application protocol of the SS7 protocol stack (cf. [4], chapter

[1] For an overview of security-related signaling of GSM and similar systems, see e.g. [1], chapter 7; more specific information can be found in [2].

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 142–152, 1999.

17).[2] If an intruder succeeds in eavesdropping these sensitive data, serious impersonation attacks or eavesdropping of user traffic on the air interface may result (cf. section 2). In addition, there are several other sensitive MAP messages. Although no attack of this kind has been reported for GSM networks to date, it is intended for UMTS to protect against these kind of attacks to achieve a constantly increased security level.

Therefore, in this document a mechanism for securing sensitive MAP messages between network elements is described. The mechanism is currently under discussion in the security group of 3GPP (Third Generation Partnership Project), a joint project of ETSI and Japanese, American, Korean and Chinese standardisation bodies working on the security specifications for UMTS.

The proposed mechanism provides confidentiality, authenticity and integrity of the messages exchanged; however, there may be messages where no confidentiality or no protection at all is needed. Therefore, three levels of protection have been defined that are applied to the various MAP messages according to their sensitivity: Protection mode 0 is identical to the original MAP message in cleartext and thus provides no protection, while protection mode 1 provides integrity and authenticity, and protection mode 2 provides confidentiality, integrity and authenticity of MAP messages.

2. The Main Threat: Compromise of Authentication Data

In mobile phone networks using a similar approach for authenticating the user as the GSM network, authentication data can get compromised, either during its transport between the home environment and the serving network, or by unauthorised access to databases. This can lead to various, serious attacks including the following:

- **Forcing use of a compromised cipher key**

The intruder obtains a sample of authentication data and uses it to convince the user that he is connected to a proper serving network, and forces the use of a compromised cipher key. The intruder may force the repeated use of the same authentication data to ensure the same encryption key will be used for many calls. This leads to continuous eavesdropping.

- **Impersonating the user**

The intruder obtains a sample of authentication data and uses it to impersonate a user towards the serving network.

Although no attacks of this kind have been reported for second generation mobile networks to date, the security level for third generation mobile systems will be increased. The security improvements comprise the access as well as the core networks [5]. The present paper concentrates on the core network security features "Entity Authentication", "Data Confidentiality" and "Data Integrity" as defined in [6],

---

[2] Note however that there are plans to have an alternative all IP based network solution for UMTS with the Release ’00. In this case, an equivalent to the MAP protocol will handle the security related information exchange. Clearly, the mechanisms presented by this document will hold accordingly.

section 5.2. In order to provide these features, a mechanism how to effectively protect authentication and other sensitive signaling data transmitted between network nodes of one operator (internal use) or between network nodes of different operators (external use) is proposed.

3. Overview of Mechanism

The proposed mechanism consists of three layers.

3.1 Layer I

Layer I is a secret key transport mechanism based on an asymmetric[3] crypto-system and is aimed at agreeing on a symmetric session key for each direction of communication between two networks X and Y. The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party may choose a symmetric session key of its own, used for sending data in the other direction. The symmetric session keys are protected by asymmetric techniques. They are exchanged between certain newly defined elements called the Key Administration Centres (KAC) of the network operators X and Y. The format of the Layer I transmissions is based on ISO/IEC 11770-3: Key Management – Mechanisms using Asymmetric Techniques [7].[4] It is proposed that public keys will be exchanged between a pair of network operators when setting up their roaming agreement.[5] In this case no general Public Key Infrastructure (PKI) is required. For the transmission of the messages, no special assumptions regarding the transport protocol are made, a possible example would be IP.

3.2 Layer II

In Layer II the agreed symmetric session keys for sending and receiving data are distributed by the KACs in each network to the relevant network elements. For example, an AuC will normally send sensitive authentication data to VLRs belonging to other networks and will therefore get a session key for sending from its KAC. Layer II is carried out entirely inside one operator's network. However, it is clear that the distribution of the symmetric keys to the network elements must be carried out in a secure way, as not to compromise the whole system.

---

[3] For UMTS a large number of network operators is expected. In this case key transport mechanisms based on asymmetric algorithms offer advantages regarding key management. Therefore, we propose to use an asymmetric scheme in Layer I.

[4] For a general overview of key transport mechanisms based on asymmetric techniques, see chapter 12.5 of [8].

[5] In general a Public Key Infrastructure is required to handle public keys and the appropriate certificates.

3.3 Layer III

Layer III uses the distributed symmetric keys for securely exchanging sensitive data between the network elements of one operator (internal use) or different operators (external use) by means of a symmetric encryption algorithm. The encrypted (resp. authenticity/integrity-protected) messages will be transported via the MAP protocol.

3.4 General Overview

Figure 1 may help to clarify the proposal by providing an overview of the whole mechanism. Note that the messages are not fully specified in this figure. Rather, only the "essential" parts of the messages are given. More details on the format of the messages in the single layers will be provided in subsequent chapters.

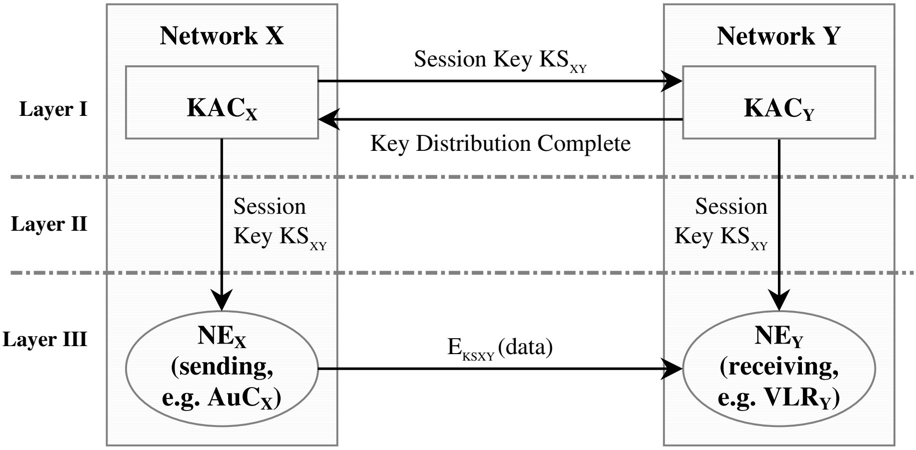


Fig. 1. Overview of proposed mechanism[6]

4. Layer I Message Format

Layer I describes the communication between two newly defined network entities belonging to different networks, the so-called Key Administration Centres (KAC). We do not make any assumptions about the protocols to be used for this communications, although IP might be the most likely candidate.

4.1 Properties and Tasks of Key Administration Centres

It is assumed that there is only one KAC per network operator. As will become evident from the following, KACs are needed to perform the following tasks:

[6] For details on the abbreviations, see the appendix.

- Generation and storage of its own asymmetric key pairs (different key pairs used for signing/verifying and encrypting/decrypting)
- Storage of public key pairs of KACs of other network operators
- Generation and storage of symmetric session keys for sending/receiving sensitive information to network entities of other networks
- Secure distribution of symmetric session keys to network entities in the same network.

Due to these sensitive tasks, a KAC has to be physically secured.

4.2 Transport of Session Keys

The transport of session keys in Layer I is based on asymmetric cryptographic techniques (cf. [8]).

In what follows, it is assumed that the involved networks have exchanged their respective public keys in course of a roaming agreement. Therefore, no public key certificates are needed.

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, KAC_X sends a message containing the following data to KAC_Y:

$$E_{PK(Y)}\{X||Y||i||KS_{XY}(i)||RND_X||Text1|| \\ D_{SK(X)}(Hash(X||Y||i||KS_{XY}(i)||RND_X||Text1))||Text2\}||Text3$$

The reasons for this message format are as follows:

- Encrypting the message with the public key of the receiving network Y (used for encrypting) provides message confidentiality, while decrypting the message body with the private key of the sending network X (used for signing) provides message integrity and authenticity.
- X includes RND_X to make sure that the message contents contains some random data before signing.

The symmetric session keys $KS_{XY}(i)$ should be periodically updated by this process, thereby moving on to $KS_{XY}(i+1)$. For each new session key KS_{XY} the version no. i is incremented by one.

After having successfully decrypted the key transport message and having verified the digital signature of the sending network including the hash value and having checked the received i the receiving network starts Layer II activities.

If anything goes wrong, e.g. computing the hash value of $X||Y||i||KS_{XY}(i)||RND_X||Text1$ does not yield the expected result, a RESEND message should be sent by Y to X in the form

$$RESEND||Y||X$$

Y shall reject messages with i smaller or equal than the currently used i.

After having successfully distributed the symmetric session key received by network X to its network entities, network Y sends to X a KEY_DIST_COMPLETE Message. This is an indication to KAC_X to start with the distribution of the key to its own entities, which can then start to use the key immediately. The message takes the form

$$KEY\_DIST\_COMPLETE \| Y \| X \| i \| RND_Y \| \\ D_{SK(Y)}(Hash(KEY\_DIST\_COMPLETE \| Y \| X \| i \| RND_Y)$$

where i indicates the distributed key and RND_Y is a random number generated by Y. Network Y includes RND_Y to make sure that the message contents determined by X will be modified before signing. The digital signature is appended for integrity and authenticity purposes.

5. Layer II Message Format

In Layer II symmetric session keys (to encrypt/decrypt data before sending/after receiving) are distributed by the KACs in each network to the relevant network elements. For example, an AuC_X will normally send sensitive authentication data to VLR_Y and will therefore get a session key KS_{XY} from its KAC_X. Layer II is carried out entirely inside one operator's network.

However, in order to achieve a more consistent overall scheme, in this section it is suggested to use for Layer II the same mechanism for distributing the keys as in Layer I. This requires the KACs of the different networks to generate and distribute asymmetric key pairs for the network elements of that network. These key pairs will then be used to transfer the symmetric session keys in the same way as in Layer I.

The public and private key pairs needed for the network entities should be distributed to the entities in a secure way, which is in principle an operation & maintenance task. One way to do this is to distribute the key pairs, along with the necessary crypto-software, to the network entities in the form of chipcards, which can also carry out the necessary computations. Therefore, all that has to be added to the present network entities are chipcard readers with a standardised interface. Thus, on adoption of this proposal, in addition to their present tasks, the network entities would have to:

- Store the symmetric session keys to encrypt/decrypt data before sending/after receiving to/from network entities of other networks (external) and of their own network (internal)
- Encrypt/decrypt MAP messages according to their mode of protection (see section 4). The necessary computations may be carried out by chipcards.

In addition to their tasks listed in section 3.1, the KACs would have to:

- Generate and store asymmetric key pairs for network entities in the same network
- Distribute asymmetric key pairs to network entities in the same network.

The Layer II messages themselves take the same form as in section 2, where the 'receiving network Y' has to be replaced by 'receiving network entity NE_X' (or X by NE_Y). Further, the Key Distribution Complete message is not needed in Layer II.

In order to ensure that no network element starts enciphering with a key that not all potentially corresponding network elements have received yet, the following approach is suggested:

The distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by the KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key.

A similar statement holds if the transported keys are used internally only: In this case, all network elements of X should get the symmetric session key KS_{XX} to be used internal for encryption (marked with flag RECEIVED) first; if all network elements have acknowledged that they have recovered these keys, the KAC_X sends the same key again (marked with flag SEND). Again, as soon as a network element has received the session key KS_{XX} (marked with flag SEND), it may start enciphering with this key.

This results in the message format described in the following.

As for layer I, no assumptions about the transport protocol are made, although IP might be a good candidate.

5.1 Sending a Session Key for Decryption

In order to transport a symmetric session key (marked with flag RECEIVE) with version no. i to be used to decrypt received data from network elements of network X in NE_Y, KAC_Y sends a message containing the following data to NE_Y:

$E_{PK(NEY)}\{X\|\|NE_Y\|\|RECEIVE\|\|i\|\|KS_{XY(i)}\|\|RND_Y\|\|Text1\|\|$ $D_{SK(Y)}(Hash(X\|\|NE_Y\|\|RECEIVE\|\|i\|\|KS_{XY}(i)\|\|RND_Y\|\|Text1))\|\|Text2\}\|\|Text3$

After having successfully decrypted the key transport message and having verified the digital signature of the sending network including the hash value, the receiving network entity sends a key installed message to its Key Administration Centre KAC_Y. The message takes the form:

$KEY\_INSTALLED\|\|X\|\|NE_Y\|\|RND_Y\|\|i$

This message can only be sent by the receiving network entity, because only this entity can know about RND_Y. If anything goes wrong, e.g. computing the hash value of $X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1$ does not yield the expected result, a RESEND message should be sent by NE_Y to KAC_Y in the form

$RESEND\|\|NE_Y$

5.2 Sending a Session Key for Encryption

In order to transport a symmetric SEND key with version no. i to be used for sending data from NE_X to network elements of network Y, KAC_X sends a message containing the following data to NE_X:

$$E_{PK(NEX)}\{NE_X\|Y\|SEND\|i\|KS_{XY}(i)\|RND_X\|Text1\|$$
$$D_{SK(X)}(Hash(NE_X\|Y\|SEND\|i\|KS_{XY}(i)\|RND_X\|Text1))\|Text2\}\|Text3$$

6. Layer III Message Format

6.1 General Structure of Layer III Messages

Layer III messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Layer III messages, three levels of protection (or protection modes) are defined providing the following security features:

Protection mode 0: no protection
Protection mode 1: integrity, authenticity
Protection mode 2: confidentiality, integrity, authenticity

Layer III messages consists of a security header and the Layer III message body. Depending on the protection mode Layer III message bodies are protected by a symmetric encryption algorithm, using the symmetric session keys that were distributed in layer II. Layer III Messages have the following structure:

Security Header	Layer III Message Body

In all three protection modes, the security header is transmitted in cleartext. It shall comprise the following information:

- Protection mode
- Other security parameters (if required, e.g. IV, version no. of key used, encryption algorithm identifier, mode of operation of encryption algorithm, etc.)

Both parts of the Layer III messages, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form:

MAP Message Header	MAP Message Body

Layer III Message

MAP Message Header	Security Header	Layer III Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Layer III message body is essentially the encrypted "old" MAP message body. For integrity and authenticity, an encrypted hash value calculated on the concatenation of MAP message header, security header and the "old" MAP message body in cleartext is included in the Layer III message body in protection modes 1 and 2. In protection mode 0 no protection is offered, therefore the Layer III message body is identical to the "old" MAP message body in cleartext in this case.

In the following subchapters, the contents of the Layer III message body for the different protection modes will be specified in greater detail.

6.2 Format of Layer III Message Body

6.2.1 Protection Mode 0

Protection mode 0 offers no protection at all. Therefore, the Layer III message body in protection mode 0 is identical to the original MAP message body in cleartext.

6.2.2 Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

$$\text{Cleartext}\|\text{TVP}\|$$
$$E_{KSXY(i)}(\text{Hash}(\text{MAP Header}\|\text{Security Header}\|\text{Cleartext}\|\text{TVP}))$$

where "Cleartext" is the message body of the original MAP message in clear.

Authentication of origin is achieved by encrypting the hash value of the cleartext by a symmetric encryption algorithm, since only a network element knowing $KS_{XY}(i)$[7] can encrypt in this way. Message integrity and validation is achieved by hashing and encrypting the cleartext.

Note that protection mode 1 is compatible to the present MAP protocol, since everything appended to the cleartext may be ignored by a receiver incapable of decrypting.

6.2.3 Protection Mode 2

The Layer III message body in protection mode 2 takes the following form:

$$E_{KSXY(i)}(\text{Cleartext}\|\text{TVP}\|\text{Hash}(\text{MAP Header}\|\text{Security Header}\|\text{Cleartext}\|\text{TVP}))$$

where "Cleartext" is the message body of the original MAP message in clear.

Message confidentiality is achieved by encrypting with the symmetric session key. This also provides for authentication of origin, since only a network element knowing $KS_{XY}(i)$ can encrypt in this way. Message integrity and validation is achieved by hashing the cleartext. TVP is a random number that avoids traceability.[8]

---

[7] The case X=Y, i.e. only one key for sending and receiving, corresponds to internal use inside network X.

[8] By using a TVP as timestamp (perhaps derived from an overall present master time) replay attacks could be avoided.

7. Discussion

7.1 Mapping of MAP Messages and Modes of Protection

It is proposed that each network operator should be able to assign the mode of protection of each MAP message in order to adapt the level of protection according to its own security policy.

7.2 Some possible problems

In protection mode 2, the original MAP message body will be encrypted in order to achieve confidentiality. For integrity and authenticity, an encrypted hash value calculated on the MAP message header and body in cleartext (i.e. the original MAP message) is appended to the messages in protection mode 1 and 2. All protection modes need a security header to be added.

When implementing these changes, care has to be taken that the maximum length of a MAP message (approx. 250 byte) is not exceeded by the protected MAP messages of Layer III, otherwise substantial changes to the underlying SS7 protocol levels (TCAP and SCCP) would have to be made.

References

[1] W. Webb: Understanding Cellular Radio, Artech House Publishers, 1998.

[2] ETSI GSM 02.09 Version 7.0.0: Security Related Network Functions.

[3] ETSI GSM 09.02 Version 7.0.0: Mobile Application Part (MAP) Specification.

[4] J.G. van Bosse: Signaling in Telecommunication Networks, John Wiley & Sons, 1998.

[5] S. Pütz: Security for the Third-Generation Mobile Radio System UMTS, Proc. of Networking the Future, 38th European Telecommunications Congress (FITCE 1999), Utrecht, Netherlands, 1999.

[6] 3GPP Technical Specification 33.102 Version 3.1.0: Security Architecture.

[7] ISO/IEC 11770 Part 3: Key Management – Mechanisms using Asymmetric Techniques, 1996.

[8] A. J. Menezes, P. C. v. Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

Appendix: Abbreviations and Proposed Key Lengths

The following abbreviations are used in this paper:

AuC	Authentication Centre
$D_{SK(X)}$(data)	Decryption of "data" with secret key of X (used for signing)
E_{KSXY}(i)(data)	Encryption of "data" with symmetric session key #i for sending data from X toY
$E_{PK(X)}$(data)	Encryption of "data" with public key of X
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communication
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
IV	Initialisation Vector
KAC_X	Key Administration Centre of network X
KS_{XX}(i)	Symmetric session key #i for sending data within network X
KS_{XY}(i)	Symmetric session key #i for sending data from X to Y
m1‖m2	Concatenation of message m1 and m2
MAP	Mobile Application Part
NE_X	Network Element of network X
RND_X	Unpredictable random value generated by X
SCCP	Signaling Connection Control Part
SS7	Signaling System No. 7
TCAP	Transaction Capabilities Applications Part
Text1	Optional data field
Text2	Optional data field
Text3	Public key algorithm identifier and public key version number (eventually included in a public key certificate)
TVP	Time Variant Parameter
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
X, Y	Network identifier

The following parameter lengths are proposed:

TVP	64 bit
RND	128 bit
X,Y	32 bit
Hash(data)	160 bit
Public Key	2048 bit
Secret Key	2048 bit
KS_{XX}, KS_{XY}	128 bit

t r’s tt c t r s c cr pt p ts

ic olas Ho gra e- ra a a d ea - ierre eifert

a he a ca Sc e ce e a e , U e f a h,
a h, Y, U
nahg@math.bath.ac.uk
e a e f a he a c , ha fga g e he U e
a f a a , e a
seifert@mi.informatik.uni-frankfurt.de

e e ha h ha he he RS c e h a ec g e e , d, h ch e ha $N^{\ /}$ a a e c g e e , e, a a e he a e e a N, he d ca a be f f he c e f ac a a f e/N e e e h a ac he ca e he he e a e a e_i f a g e N, a h a d_i he ca e f ch e_i, he d_i ca he ca be a a ge a $N^{\ /}$ a be effic e ec e e he be f e c g e e c ea e he b he d_i, h ch e ab e effic e ec e f he d_i, c ea e $N^{\ -\epsilon}$ e e , he c e f e h e e a he be f e e e e , a he ef e ac ca f a e a e a be f he

tr ct

I t e protocol (see [ ]), lice p lis es a p lic od l s N a d a e cr pti g e po e t e. e od l s N s o ld e t e prod ct of t o large disti ct pri es p a d q ic are kept secret. o ake t e factori g of N ard, p a d q are ofte c ose it a o t t e sa e er of digits. it t e k o ledge of p a d q lice ca also calc late d s c t at $ed =$ od $\lambda(N)$ ere $\lambda(N) =$ lc $(p-\ ,q-\ )$. o e is i g to e cr pt a essage m for lice t e raises it to t e po er e od lo N. is ca t e e decr pted (opef ll o l lice) a ot er e po e tiatio si ce $(m^e)^d = m$ (od N). learl if o e ca factor N t e o e ca also decr pt a essages se t to lice.

espite t e t ears of i te si e researc o t e cr ptos ste o de- astati g attacks o it a e ee disco ered so far. Ho e er, der certai cir- c sta ces ore efficie t attacks rat er t a si pl factori g t e od l s N are k o (see o e [ ] for a rece t s r e). e of t ose is t e se of a s all pri ate e po e t d a d a ot er o e is t e se of a co o od l s N for se eral ke pairs e_i, d_i. et s ela orate t ese attacks a little it f rt er.

or efficie t sig at re ge eratio it a e te pti g to se a s all pri ate e po e t d. U fort atel , ie er [ ] as s o t at e t e protocol is sed it a decr pti g e po e t, d, less t a $N^{\ /}$ a d a e cr pti g

e po e t, e, appro i atel t e sa e si e as N, t e t e s ste ca e roke . er rece tl o e a d rfee [ ] a aged to i pro e ie er's res lt s o i g o to reak t e s ste e e e si g decr pti g e po e ts of si e less t a $N^{\cdot}$. I order to si plif t e ke a age e t o e a e te pted to se a si gle od l s for se eral ke pairs e_i, d_i. Ho e er, as poi ted o t i o s [i], e e er a essage m is se t to t o participa ts ose p lic e po e ts appe to e relati el pri e, t e t e essage m ca e easil reco ered it o t reaki g t e s ste . e a re tis [ ] descri ed t o f rt er attacks i ic a participa t ca reak s c a co o od l s cr ptos ste . artic larl , e s o ed t at k o ledge of o e ke pair e_i, d_i gi es rise to a efficie t pro a ilistic algorit for factori g t e od l s N. oreo er, e also s o ed t at k o ledge of o e ke pair e_i, d_i gi es rise to a efficie t deter i istic algorit to ge erate ot er ke pairs it o t deter i i g $\lambda(N)$. or a t oro g disc ssio of t e co o od l s sit atio e si g e refer to oore [ ].

Ho e er, e stress t at i o s attack does ot reak t e s ste at all a d t at t e attack of e a re tis ass es t at t e attacker is also gi e t e secret e po e t. Ha i g said all t is, it see s to e at ral to st d t e ore realistic pro le of at a oppo e t ig t do, gi e o l se eral p lic e po e ts for a gi e od l s a d t e k o ledge of t e correspo di g pri ate e po e ts ei g q ite s all. is is t e p rpose of t is paper. lt o g , as e plai ed efore, t is sit atio is ot co o i prese t-da s ste s, a a al sis of t is pro le s eds so e lig t o t e gai of additio al p lic i for atio i attacki g a d o t e sec rit of re- si g t e od l s N. oreo er, it see s a at ral a to etter dersta d a d e te d ie er's origi al idea ic ig t also e sef l i ot er circ sta ces.

e q estio of o to co i e se eral p lic e po e ts for a gi e od l s i order to red ce t e si e co strai t o t e pri ate e po e ts for t eir efficie t reco str ctio as o l er rece tl i itiated o [ ]. till ased o t e co ti ed fractio approac of ie er, o s o ed o to reak gi e 3 p lic e po e e ts e e e t eir correspo di g decr pti g e po e ts are of si e less t a $N^{\ /}$. Usi g i stead a lattice asis red ctio approac e co ti- e t is st d ere, ge eralisi g (a d i pro i g) t e res lt p to a ar itrar er of e po e ts. artic larl , e s o t at it n e cr pti g e po e ts e_i, o r lattice asis approac allo s for t e d_i to e as large as N^{α_n} ere

$$\alpha_n = \begin{cases} \dfrac{(\ n\ \ )^{\ n}-(\ n\ \ )\binom{n}{n/\ }}{(\ n-\ )^{\ n}\ \ (\ n\ \ )\binom{n}{n/\ }} & \text{if } n \text{ is e e ,} \\[2ex] \dfrac{(\ n\ \ )^{\ n}-\ n\binom{n-}{n-\ \ /\ }}{(\ n-\ )^{\ n}\ \ n\binom{n-}{n-\ \ /\ }} & \text{if } n \text{ is odd.} \end{cases}$$

It is i teresti g to ote t at o r et od alread allo s for 2 e cr pti g e - po e ts a decr pti g e po e t o d of $N^{\ /}$, ic is s perior to t e $N^{\ /}$ o d of o for 3 e cr pti g e po e ts.

s o r approac co i es ideas fro ot ie er a d o i to a si gle lattice t e e t sectio re ie s t e approac es of ie er a d o a d gi es

a o er ie of o r e te sio approac . r sol tio to t e ge eral pro le of n e cr pti g e po e ts is gi e i sectio 3 starti g it so e preli i aries a d e a i i g first t e cases of 2, 3 a d 4 e po e ts efore ge eralisi g t e approac to n e po e ts. ectio 4 t e descri es e peri e tal res lts for o r lattice asis.

r t p t tt c s

. i r's ppr c

It as s o i ie er [ ] t at, if o e ass es $\lambda(N)$ a d e are ot appro i- atel as large as N, a d if t e decr pti g e po e t d is less t a $N^{\ /}$ t e t e od l s N ca e factored e a i i g t e co ti ed fractio appro i atio of e/N. is follo s eca se e a d d satisf t e relatio s ip $ed - k\lambda(N) =$. o letti g $\lambda(N) = (p - \ )(q - \ )/g$, a d $s = \ - p - q$ e a e t at

$$edg - kN = g + ks. \qquad (\ )$$

i idi g ot sides dgN gi es

$$\frac{e}{N} - \frac{k}{dg} = \frac{g + ks}{dgN} = \frac{k}{dg} \quad \frac{s}{N} + \frac{}{dN}.$$

o si g t e ass ptio t at e N, a d t at s $N^{\ /}$ ea s (fro e - a i i g eq atio) t at $k/(dg)$ so t at t e rig t- a d side of t e a o e eq atio is appro i atel $N^{-\ /}$. It is ell k o (see for i sta ce [H]) t at if

$$x - a/b < \ /(2b\ )$$

t e a/b is a co ti ed fractio appro i a t of x. s if $N^{-\ /} < \ /(2(dg)\ )$ t e $k/(dg)$ ill e a co ti ed fractio appro i a t of e/N. is is tr e e- e er

$$d < 2^{-\ /}\ (\ /g)N^{\ /}\ , \qquad (2)$$

a d g ill e s all der t e ass ptio t at $\lambda(N)$ N (t o g clearl g 2 si ce ot p a d q are odd). i e dg o e a calc late

$$r = (p - \ )(q - \ ) = \frac{edg}{k} - \frac{g}{k} = \ edg/k \qquad (\text{si ce } g \text{ is s all}),$$

a d t e e ca factor N si ce t e factors p a d q satisf t e q adratic relati- o s ip $x\ - (N + \ - r)x + N =$.

. u 's ppr c

e approac take i o [ ] ass es t at o e as ore t a o e e_i for a gi e N, a d t at eac of t ese e_i as a relati el s all d_i. o o l co siders t e pro le for 2 a d 3 e cr ptio e po e ts. or 2 e po e ts e a e t e follo i g relatio s:

$$e\ d\ g - k\ (p - \ )(q - \ ) = g$$
$$e\ d\ g - k\ (p - \ )(q - \ ) = g,$$

so ltipl i g t e first k , t e seco d k , a d s tracti g gi es

$$k\ d\ e\ - k\ d\ e\ = k\ - k\ . \tag{3}$$

i idi g o ot sides of eq atio 3 $k\ d\ e$ i plies t e follo i g

$$\frac{e}{e} - \frac{k\ d}{k\ d} = \frac{k\ - k}{k\ d\ e},$$

a d ass i g t at t e d_i (a d e ce k_i if t e e_i are large) are at ost N^{α} ea s t at t e rig t- a d side is a o t $N^{-(\ \alpha)}$.

or t e fractio $k\ d\ /(k\ d\ )$ to e a co ti ed fractio appro i a t of $e\ /e$, e st t erefore a e t at

$$2(k\ d\ )\ < N\ ^{\alpha},$$

a d it t e ass ptio s t at k a d d are at ost N^{α} a d t at g is s all t is co ditio ill e tr e e e er $\alpha = \ /3 - \epsilon$ for so e $\epsilon >$.

Ho e er, like t e sit atio it ie er's attack, t e fractio $k\ d\ /(k\ d\ )$ does ot reak t e cr ptos ste for t o reaso s:

irstl k o i g, sa , t e erator $k\ d$, does ot allo s to fi d d or k it o t factori g t is er.

eco dl t ere a e a factor i co o et ee $d\ k$ a d $d\ k$ i ic case t e co ti ed fractio et od o ld ot gi e a fractio it erator $k\ d$ a d de o i ator $k\ d$, t rat er t e fractio it t e co o factor re o ed.

o ass es t at t e seco d pro le does ot e ist, i.e. t at e a e gcd$(k\ d\ , k\ d\ ) =$, a d it is esti ated t at t is appe s it pro a ilit $6/\pi$ .6 .

o get aro d t e first pro le , o s ggests t at o e co ld eit er tr to factor $k\ d$ (a er of si e a o t $N\ ^{/}$ a d ot t picall of a ard factorisatio s ape), or alter ati el ass e t at o e as a ot er e cr pti g e po e t e it $d\ < N\ ^{/}$. e (repeati g t e a o e proced re it e a d e) o e ca also fi d $k\ d$, a d calc lati g gcd$(k\ d\ , k\ d\ )$ ill opef ll (if gcd$(k\ , k\ ) =$) gi e d a d t s allo t e factori g of N. e pro a ilit of t is attack orki g der t e gi e ass ptio s is $(6/\pi\ )$ .23.

.3 r i ur t si ppr c

s alread said i t e i trod ctio , o r approac also ass es t at e a e ore t a o e e_i for a gi e N, a d t at eac of t ese e_i as a relati el s all d_i.

I t e re ai der e ill se, a o g ot ers, ideas fro ot ie er a d o to sol e t e ge eral pro le of reaki g i t e prese ce of n e cr pti g e - po e ts e_i, all it relati el s all $d_i < N^{\alpha_n}$, $i =$ $, \ldots, n$. e ai tec iq e sed i deri i g t ese res lts is t e creatio a d s seq e t red ctio of certai lattices. e approac take s, o e er, ca c rre tl o l e classed as a e ristic et od eca se, alt o g t e ectors e searc for ca e s o to e relati el s ort, e ca ot pro e et t at t e are i deed a o g t e s ortest ectors (a d e ce o d to e fo d lattice asis red ctio algorit s). e- ert eless, i sectio 4 it is s o t at o r approac perfor s ell i practice, a d t at t e follo i g t eoreticall deri ed o ds are freq e tl ac ie ed. I partic lar, i t e prese ce of n e cr pti g e po e ts e_i, o r approac allo s for t e d_i to e as large as N^{α_n} ere

$$\alpha_n = \begin{cases} \frac{(n \quad) ^{n} - (n \quad) \binom{n}{n/}}{(n- \;) ^{n} \quad (n \quad) \binom{n}{n/}} & \text{if } n \text{ is e e ,} \\ \frac{(n \quad) ^{n} - \; n \binom{n-}{n- \; /}}{(n- \;) ^{n} \quad n \binom{n-}{n- \; /}} & \text{if } n \text{ is odd.} \end{cases}$$

e first fe (fro $n =$) start /4, 5/ 4, 2/5, 5/34, 29/62. I sectio 3.5 it is s o t at α_n as n .

If t e algorit (see [ ]) is sed i order to red ce t e lattices derl i g o r approac , a d t e (pessi istic) esti ate for its co ple it of $O(m \;\log\; B)$ is ass ed (gi e a lattice of di e sio m it largest or B), t e t e co ple it of o r et od is $O(2 \;^{n} n \;\log\; N)$, a d so clearl t e attack is o l practical for s all n.

3 t s t r s c ll cr pt p ts

3. r li i ri s

I e te di g t e a al sis to n e cr pti g e po e ts e_i (it s all decr pti g e po e ts d_i), e se ot ie er's a d o's ideas. e s all refer to relatio s of t e for

$$d_i g e_i - k_i N = g + k_i s$$

as ie er eq atio s, a d e s all de ote t e W_i (see eq atio for a e a - ple). i ilarl e s all refer to relatio s of t e for

$$k_i d_j e_j - k_j d_i e_i = k_i - k_j$$

as o eq atio s, a d s all de ote t e $G_{i,j}$ (see eq atio 3 for a e a ple). e s all also ass e, for a gi e n, t at t e d_i a d k_i are at ost N^{α_n}, t at g is s all, a d t at s is aro d $N^{\ /\ }$. otice t at t e rig t- a d sides of W_i a d $G_{i,j}$ are t erefore q ite s all; i fact at ost $N^{(\ /\ )\ \ \alpha_n}$, a d N^{α_n} respecti el . i all e ofte refer to co posite relatio s, e.g. $W_u G_{v,w}$, i ic case e ea t e relatio , ose left- a d (resp. rig t- a d) side is t e prod ct of t e left- a d (resp. rig t- a d) sides of W_u a d $G_{v,w}$. or e a ple, $W_u G_{v,w}$ ic as a relati el s all rig t- a d side, o ded i si e $N^{(\ /\ )\ \ \alpha_n}$.

I t e follo i g a al sis e e a i e t e cases of 2, 3 a d 4 e po e ts efore ge eralisi g t e approac to n e po e ts. is is do e ot to gi e e plicit e a ples of t e approac e i t e prese ce of a s all er of e po e ts, a d also eca se it is ot til t e prese ce of 4 e po e ts t at t e ge eral p e o e o eco es clear. e relatio s t at e c oose for t e cases of 2, 3 a d 4 e po e ts a see "pl cked fro t e air", t t e patter is ade clear i sectio 3.5.

3. i t r s c ll cr pti p ts

ss i g t at e a e t o s all decr ptio e po e ts, t e t e follo i g relatio s old: W , G , , W W ; or ore e plicitl :

$$d\ ge\ \ -k\ N = g + k\ s,$$
$$k\ d\ e\ \ -k\ d\ e\ \ = k\ \ -k\ ,$$
$$d\ d\ g\ e\ e\ \ -d\ gk\ e\ N - d\ gk\ e\ N + k\ k\ k\ N\ \ = (g + k\ s)(g + k\ s).$$

ltipl i g t e first of t ese k ea s t at t e left- a d sides are all i ter s of $d\ d\ g$, $d\ gk$, $d\ gk$, a d $k\ k$, a d e ce e a rite t ese eq atio s i t e atri for elo .

$$(k\ k\ , d\ gk\ , d\ gk\ , d\ d\ g\ ) \begin{matrix} -N & & N \\ e & -e & -e\ N \\ & e & -e\ N \\ & & e\ e \end{matrix} =$$

$$(k\ k\ , k\ (g + k\ s), g(k\ \ - k\ ), (g + k\ s)(g + k\ s).$$

e si e of t e e tries of t e ector o t e rig t- a d side are at ost $N^{\ \alpha}$, $N^{(\ /\ )\ \ \alpha}$, N^{α}, a d $N^{\ \ \alpha}$ respecti el . ese si e esti ates a e ade ro g l eq i ale t ltipl i g t e first t ree col s of t e atri N, $M\ = N^{\ /\ }$, a d $M\ = N^{\ \ \alpha}$ respecti el , ic gi es t e follo i g atri :

$$L\ = \begin{matrix} N & -M\ N & & N \\ & M\ e & -M\ e & -e\ N \\ & & M\ e & -e\ N \\ & & & e\ e \end{matrix}$$

I t is case t e ector $b = (k\ k\ , d\ gk\ , d\ gk\ , d\ d\ g\ )$ ill e s c t at

$$bL\ \ < 2N^{\ \ \alpha}.$$

e st o ake t e ass ptio t at, i t e lattice ge erated t e ro s of L , t e s ortest ector as le gt $\Delta^{/ -\epsilon}$, ere $\Delta := \det(L\ )$ $N^{(\ /\ )\ \alpha}$, a d oreo er t at t e e t s ortest li earl i depe de t ector as a sig ifica tl larger or t a t e s ortest ector i L . I deed, if t e lattice L is prett "ra do ", t ere are al ost s rel o lattice poi ts of L sig ifica tl s orter t a t e i ko ski o d $2\Delta^{/}$. U der t ese ass ptio s, t e bL is t e s ortest ector i t e lattice if

$$N\ \ ^{\alpha} < (\ /c\ )\ N^{(\ /\ )\ \alpha}\ \ ^{/}$$

for so e s all c , ic is tr e if

$$\alpha\ < 5/\ 4 - \epsilon\ .$$

is i plies t at t e ector $b = (b\ , b\ , b\ , b\ )$ ca e fo d ia lattice asis red ctio algorit s (e.g.) if $\alpha\ < 5/\ 4 - \epsilon$, a d t e $d\ g/k\ = b\ /b$ ca e calc lated, ic leads to t e factori g of N as s o i sectio 2. .

3.3 i t r s c 3 ll cr pti p ts

is et od e te ds easil to 3 e cr pti g e po e ts. e o a e t e q a tities $, e\ , e\ , e\ e\ , e\ , e\ e$ a d $e\ e\ e$ fro ic to for li ear relatio s ips, a d e alread a e relatio s ips co cer i g t e first fo r of t ese fro t e 2 e po e t case, a el $, W\ , G\ ,$ a d $W\ W$. or t e re ai i g relatio s ips e c oose $G\ ,\ , W\ G\ ,\ , W\ G\ ,$ a d $W\ W\ W$. ese relatio s i pl looki g for t e ector

$$b = (k\ k\ k\ , d\ gk\ k\ , k\ d\ gk\ , d\ d\ g\ k\ ,$$
$$k\ k\ d\ g, k\ d\ g, k\ d\ g, d\ d\ d\ g\ ),$$

red ci g t e ro s of t e follo i g lattice:

$$L\ = \begin{array}{cccccccc} -N & N & & & & & -N & \\ e & -e & -e\ N\ -e & & & e\ N & e\ N & \\ & e & -e\ N & & e\ N & & e\ N & \\ & & e\ e & & -e\ e & -e\ e & -e\ e\ N & \\ & & & e & -e\ N & -e\ N & e\ N & \\ & & & & e\ e & & -e\ e\ N & \\ & & & & & e\ e & -e\ e\ N & \\ & & & & & & e\ e\ e & \end{array} D,$$

ere D is t e diago al atri

$$\mathrm{diag}(N^{\ /}\ , N, N^{(\ /\ )\ \ \alpha}\ , N^{\ /}\ , N^{(\ /\ )\ \ \alpha}\ , N\ \ ^{\alpha}\ , N\ \ ^{\alpha}\ ,\ \ )$$

sed to a i ise t e deter i a t of L a d still keep

$$bL\ \ < \ ^{-}N^{(\ /\ )\ \ \alpha}\ .$$

gai , si g t e ass ptio s t at t e s ortest ector i t e lattice ge erated t e ro s of L as le gt $\det(L\ )^{(\ /\ )-\epsilon}$, a d is also sig ifica tl s orter t a t e e t s ortest li earl i depe de t ector i L , ea s t at bL ill e t e s ortest ector i t e lattice L if

$$N^{(\ /\ )\quad\alpha} < (\ /c\ )\left(N \quad \alpha \quad /\right.$$

for so e s all c ic is tr e if

$$\alpha\ < 2/5-\epsilon\ .$$

si g agai t e first t o co po e ts of b, as i t e 2 e po e t case, o e a o factor t e od l s N as s o i sectio 2. .

3. i t r s c ll cr pti p ts

I t e prese ce of 4 e po e ts e ca o se li ear relatio s ips a o g t e q a tities $,e\ ,e\ ,e\ e\ ,e\ ,e\ e\ ,e\ e\ ,e\ e\ e\ ,e\ ,e\ e\ ,e\ e\ ,e\ e\ ,e\ e\ e\ ,e\ e\ e\ ,$ $e\ e\ e$ a d $e\ e\ e\ e$. s efore e alread a e li ear relatio s ips for t e first alf of t ese q a tities fro t e a al sis i t e prese ce of 3 eq atio s. or t e re ai i g q a tities e se t e relatio s $G\ ,\ , W\ G\ ,\ , G\ ,\ G\ ,\ , G\ ,\ G\ ,\ ,$ $W\ W\ G\ ,\ , W\ W\ G\ ,\ , W\ W\ G\ ,$ a d $W\ W\ W\ W\ W$. tti g t ese relatio s i atri for , a d ltipl i g t e col s appropriate factors to ake all t e relatio s of si e at ost $N \quad \alpha$, res lts i a 6 6 atri , L , ic as deter i a t $N^{(\quad /\ )\quad\alpha}$. e ector b e are o looki g for is

$$\begin{aligned} b = (&k\ k\ k\ k\ ,d\ gk\ k\ k\ ,k\ d\ gk\ k\ ,d\ d\ g\ k\ k\ ,\\ &k\ k\ d\ gk\ ,d\ k\ d\ g\ k\ ,k\ d\ d\ g\ k\ ,d\ d\ d\ g\ k\ ,\\ &k\ k\ k\ d\ g,d\ k\ k\ d\ g\ ,k\ d\ k\ d\ g\ ,k\ k\ d\ d\ g\ ,\\ &d\ d\ k\ d\ g\ ,d\ k\ d\ d\ g\ ,k\ d\ d\ d\ g\ ,d\ d\ d\ d\ g\ ). \end{aligned}$$

erefore, agai aki g t e sa e ass ptio s as efore, i plies t at t e ector bL is t e s ortest ector i t e lattice ge erated t e ro s of L if

$$N \quad \alpha < (\ /c\ )\ \ N^{(\quad /\ )\quad\alpha} \quad /$$

for so e s all c , a d t is is tr e if

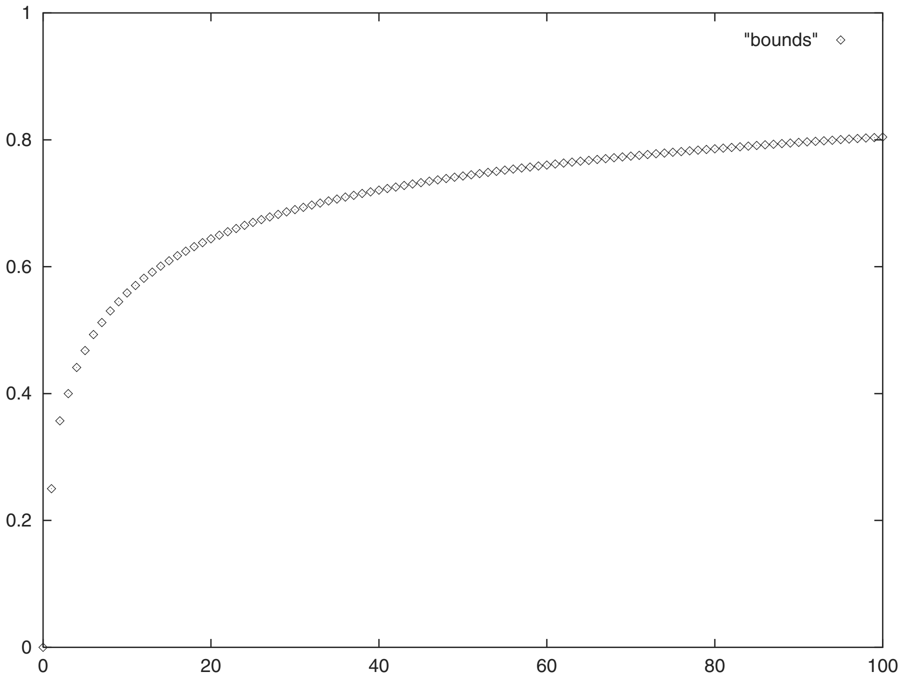
$$\alpha\ <\ \ 5/34-\epsilon\ .$$

Usi g agai t e first t o co po e ts of b, as i t e 2 a d 3 e po e t case, o e a agai factor t e od l s N as s o i sectio 2. .

3. r l ppr c

e to space li itatio s e defer t e s tle co p tatio of t e ge eral allo a le o d o t e d_i e e a e n e cr pti g e po e ts e_i, $i =$ $, \ldots, n$, to t e appe di a d s o elo si pl t e grap for

$$\alpha_n = \begin{cases} \frac{(n \quad)^{\ n} - (n \quad) \binom{n}{n/}}{(n- \quad)^{\ n} \quad (n \quad) \binom{n}{n/}} & \text{if } n \text{ is e e ,} \\ \frac{(n \quad)^{\ n} - \ n \binom{n-}{n- \quad /}}{(n- \quad)^{\ n} \quad n \binom{n-}{n- \quad /}} & \text{if } n \text{ is odd.} \end{cases}$$



ig. . rap of o ds α_n for n .

4 r ct c l s lts

lt o g o r et od is at t e c rre t ti e o l e ristic, it orks ell i practice as ca e see fro o r e peri e tal res lts elo .

r i ple e tatio ses t e li rar [ ] of ictor o p. i i gs are gi e for a 3 H K6 r i g der i .

- t c ts			
α	it le gt of d_i	a g. ti e i secs.	s ccess rate
.356	7	.44	4 %
.354	77	.42	%

ig. 2. erage r i g ti e (i seco ds) a d s ccess rate for ra do e peri e ts as a f ctio of α .

- t c ts			
α	it le gt of d_i	a g. ti e i secs.	s ccess rate
.357 43	25	. 75	%
.3557 4	249	. 7	7 %
.3542 6	24	.93	%
.352 57	247	.33	%

ig. 3. erage r i g ti e (i seco ds) a d er of s ccess rate for ra do e peri e ts as a f ctio of α .

- t 3 c ts			
α	it le gt of d_i	a g. ti e i secs.	s ccess rate
.4	2	3.632	%
.39	99	3.567	4 %
.396	9	3.599	9 %
.394	97	3.726	9 %
.392	96	3.595	9 %
.39	95	3.529	%

ig. 4. erage r i g ti e (i seco ds) a d s ccess rate for ra do e peri e ts as a f ctio of α .

- t c ts			
α	it le gt of d_i	a g. ti e i secs.	s ccess rate
.44		4.53	%
.435	7	4.496	5 %
.43	6	4.32	%
.425	5	4. 59	%

ig. 5. erage r i g ti e (i seco ds) a d s ccess rate for ra do e peri e ts as a f ctio of α .

- t c ts			
α	it le gt of d_i	a g. ti e i secs.	s ccess rate
.45	9	424.756	%
.445	9	427.275	6 %
.44		422.74	%

ig. 6. erage r i g ti e (i seco ds) a d s ccess rate for ra do e peri e ts as a f ctio of α .

p r l s

e ajor ope pro le raised o r ork is t e follo i g. o ork o t t e a agea le o d o α_n for t e secret e po e ts e ad to ake t o e ristic ass ptio s co cer i g “ra do ” lattices. s t e e peri e tal res lts stro gl s pport t e deri ed o ds it is at ral to ask et er o r attack ca e t r ed i to a rigoro s t eore ?

r c s

eh, T e ea f a ac RS , *i s f h* 4 , ,

eh, fee, e e he c a a f e e RS , a ea *r . f Y ’*

e a e , f he ea e he c c f he RS c a g h , *r gi* 8, 5 5 , 84

R , a ca f ha e a a c e ec , a ea *h i s f i n*

a , E gh , *n in r d i n h h r f n rs,* 5 e , f U e P e ,

e a, e a, a , ac g a h ege c effic e , *h is h nn n* , 5 5 4, 8

e, P c fa e c e , S e , *n- r r r g* , EEE P e ,

RS R R e , Sha , e a , e h f b a g g a g a e a b c e c e , *n.* , , 8

Sh Sh , be The b a T , `http://www.cs.wisc.edu/~shoup.ntl`

S S , ea ac c g he RS c a g h , *r - gi* , 8 8 , 8

T E R e he , a T b g, a a f e Sh RS ec e e e , *i g r in ng n ring ni i n nd - ing* 8, 4 5 4 5,

e e , a a f h RS e e , *r ns. n nf r i n h r* , 55 558,

pp

e o ork o t t e ge eral o d o t e d_i e e a e n e cr pti g e po e ts. e reader is e co raged to refer ack to t e pre io s sectio s (e $n = 2, 3$ a d 4) as e a ples.

i e t at t ere are n e po e ts e_i, t e t ere are 2^n differe t q a tities, h_j, i ol i g t e e_i’s, a d t e prod ct of all of t ese (ass i g e N) is $N^{(n \;\; n-\;\;)}$. is ea s t at o e co siders a diago al atri , L_n, of di e sio 2^n, a d t at t e deter i a t of t is atri , efore ltipl i g t e ro s to i crease t e allo a le o d, is $N^{(n \;\; n-\;\;)}$.

e last relatio $W W \ldots W_n$ as a rig t- a d side of at ost $N^{(n/\ )\ n\alpha_n}$, a d t s e i crease t e rig t- a d side of all t e ot er relatio s p to t is o d, aki g t e desired ector b s c t at bL_n is (still) appro i atel $N^{(n/\ )\ n\alpha_n}$. e ge eral for of t e desired ector b is t at its j h e tr is t e prod ct of n k o q a titities a_i for $i = \ \ldots n$, ere a_i is eit er $d_i g$ or k_i depe di g o et er e_i is prese t i t e j h q a tit h_j or ot.

e o co sider t e i teresti g pro le of ic relatio s to co sider for n eq atio s. ser e t at a ge eral relatio of t e for

$$R_{u,v} = W_i \ \ldots W_{i_u} G_{j\ ,l}\ \ldots G_{j_v,l_v},$$

(ere t e $i\ ,\ldots,i_u, j\ ,\ldots,j_v, l\ ,\ldots,l_v$ are iq e), as a left- a d side co -posed of prod cts of $(u+2v)$ of t e e_i's it coefficie ts t at are prod cts of $(u+v)$ of t e k o q a tities a_i (ere a_i is agai eit er $d_i g$ or k_i). lso otice t at t e rig t- a d side of $R_{u,v}$ as si e at ost $N^{(u/\ )\ (u\ \ v)\alpha_n}$.

r et od req ires all t e coefficie ts to e ro g l t e sa e si e (a prod ct of n of t e q a tities a_i). is ea s t at relatio s ic a e coefficie ts less t a t is st e ltiplied (o ot sides) so e issi g k_i. or e a ple, i t e t e 2 e po e t case e ltiplied t e first eq atio k to ake all t e coefficie ts of si e $N^{\ \alpha}$. is as t e effect of i creasi g t e rig t- a d side of relatio $R_{u,v}$ to a si e o ded $N^{(u/\ )\ (n-v)\alpha_n}$.

i e t is e relatio $R_{u,v}$ e o eed to ake it's rig t- a d side as large as t e rig t- a d side of $W W \ldots W_n$, ic ea s ltipl i g (ot sides) $N^{(n-u)/\ \ v\alpha_n}$. or e a ple, t ese ltiplicatio factors are t e (diago al) e tries of t e diago al atri D i t e e a ple e $n = 3$.

a t at t e prod ct of t ese ltiplicatio factors (i.e. t e deter i a t of D i t e $n = 3$ e a ple) is N^{β_n}, ere $\beta_n = x + y\alpha_n$, a d let L_n de oted t e lattice of (odified) relatio s as efore. is ea s t at (der t e s al ass ptio s) t e ector bL_n is t e s ortest ector of t e lattice if

$$N^{n/\ \ n\alpha_n} < (\ /c_n)\ N^{n\ \ n-\ \ \ x\ \ y\alpha_n\ \ \ /\ n}$$

for so e s all c_n, i.e. e

$$\alpha_n < \frac{x}{n2^n - y} - \epsilon\ . \tag{4}$$

I order to a i ise α_n e is ot x a d y to e large. is ea s t at t e relatio s s o ld e c ose to a i ise v (a d i i ise u). or i sta ce e $n = 2$ e c oose t e relatio s $W\ , G\ _,$ a d $W W$ rat er t a $W\ , W$ a d $W W$ eca se $\beta\ = 2$ i t e latter case rat er t a $5/2 + \alpha$ i t e for er.

it t is ge eral pri ciple i i d e still eed to e plai e actl ic relatio s e se. I order to a tai t e tria g larit of L_n e o l co sider relatio s ic i trod ce o e e q a tit h_j. e c oices for n 5 ca e see i t e elo fig re.

h_j	relatio	si e of coeffs	si e of h_j	si e of r s	co tri tio to β_n
	–				$(n/2)$
e	W			$(/2)+\alpha_n$	$(n-)/2$
e	$G_{,}$	2		α_n	$(n/2)+\alpha_n$
$e\ e$	$W\ W$	2	2	$+2\alpha_n$	$(n-2)/2$
e	$G_{,}$	2		α_n	$(n/2)+\alpha_n$
$e\ e$	$W\ G_{,}$	3	2	$(/2)+2\alpha_n$	$(n-)/2+\alpha_n$
$e\ e$	$W\ G_{,}$	3	2	$(/2)+2\alpha_n$	$(n-)/2+\alpha_n$
$e\ e\ e$	$W\ W\ W$	3	3	$(3/2)+3\alpha_n$	$(n-3)/2$
e	$G_{,}$	2		α_n	$(n/2)+\alpha_n$
$e\ e$	$W\ G_{,}$	3	2	$(/2)+2\alpha_n$	$(n-)/2+\alpha_n$
$e\ e$	$G_{,}\ G_{,}$	4	2	$2\alpha_n$	$(n/2)+2\alpha_n$
$e\ e$	$G_{,}\ G_{,}$	4	2	$2\alpha_n$	$(n/2)+2\alpha_n$
$e\ e\ e$	$W\ W\ G_{,}$	4	3	$+3\alpha_n$	$(n-2)/2+\alpha_n$
$e\ e\ e$	$W\ W\ G_{,}$	4	3	$+3\alpha_n$	$(n-2)/2+\alpha_n$
$e\ e\ e$	$W\ W\ G_{,}$	4	3	$+3\alpha_n$	$(n-2)/2+\alpha_n$
$e\ e\ e\ e$	$W\ W\ W\ W$	4	4	$2+4\alpha_n$	$(n-4)/2$
e	$G_{,}$	2		α_n	$(n/2)+\alpha_n$
$e\ e$	$W\ G_{,}$	3	2	$(/2)+2\alpha_n$	$(n-)/2+\alpha_n$
$e\ e$	$G_{,}\ G_{,}$	4	2	$2\alpha_n$	$(n/2)+2\alpha_n$
$e\ e$	$G_{,}\ G_{,}$	4	2	$2\alpha_n$	$(n/2)+2\alpha_n$
$e\ e$	$G_{,}\ G_{,}$	4	2	$2\alpha_n$	$(n-2)/2+\alpha_n$
$e\ e\ e$	$W\ W\ G_{,}$	4	3	$+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e$	$W\ G_{,}\ G_{,}$	5	3	$(/2)+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e$	$W\ G_{,}\ G_{,}$	5	3	$(/2)+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e$	$W\ G_{,}\ G_{,}$	5	3	$(/2)+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e$	$W\ G_{,}\ G_{,}$	5	3	$(/2)+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e$	$W\ G_{,}\ G_{,}$	5	3	$(/2)+3\alpha_n$	$(n-)/2+2\alpha_n$
$e\ e\ e\ e$	$W\ W\ W\ G_{,}$	5	4	$(3/2)+4\alpha_n$	$(n-3)/2+\alpha_n$
$e\ e\ e\ e$	$W\ W\ W\ G_{,}$	5	4	$(3/2)+4\alpha_n$	$(n-3)/2+\alpha_n$
$e\ e\ e\ e$	$W\ W\ W\ G_{,}$	5	4	$(3/2)+4\alpha_n$	$(n-3)/2+\alpha_n$
$e\ e\ e\ e$	$W\ W\ W\ G_{,}$	5	4	$(3/2)+4\alpha_n$	$(n-3)/2+\alpha_n$
$e\ e\ e\ e\ e$	$W\ W\ W\ W\ W$	5	5	$(5/2)+5\alpha_n$	$(n-5)/2$

ta le s o i g t e c ose relatio s for n 5.

fter t e i itial " ase relatio " (ic req ires t at t e first co po e t of b s o ld e s all), e seek a li ear relatio et ee e a d (or a ltiple of t is e.g. N), a d o r o l c oice for t is is W. it t e i trod ctio of t e e t e po e t e e o look for a relatio et ee , e a d e . or t is e ca eit er c oose W or $G_{,}$, a d as e plai ed a o e $G_{,}$ is t e rig t c oice.

ore i teresti g sit atio arises e t e fo rt e po e t e as ee i trod ced, a d o e looks for a relatio regardi g $e\ e$ a d t e pre io s o es. e est c oice i t is case t r s o t to e $W\ G\ _{,}$. Ho e er, e co sideri g t e e t relatio regardi g $e\ e$ a d t e pre io s o es e a o se $G\ _{,}\ G\ _{,}$ eca se t e left- a d side of t is relatio co tai s $e\ e$, $e\ e$, $e\ e$ a d $e\ e$ all of ic are o prese t.

I ge eral e looki g for a relatio regardi g $e_i\ e_i\ \ldots e_{i_s}$ a d t e pre io s o es, o e ca se a relatio $R_{u,v}$ ere $u+v=s$, s ject to t e req ired h_j ei g prese t earlier. It ca e s o t at t e er of relatio s $R_{u\ v}$ it $v=t$ s o ld e $\binom{n}{t} - \binom{n}{t-}$ regardless of t e si e $s=u+v$ of t e relatio (t o g of co rse t is is s ject to t s a d $s+2t$ n). e co tri tio to β_n for s c a relatio is $(n-s+t)/2+t\alpha_n$, a d t s (s i g o er t e possi le n) t e total co tri tio to β_n is s o elo .

$$\beta_n = \sum_{s=}^{n} \sum_{t=}^{(s,n-s)} \left(\binom{n}{t} - \binom{n}{t-} \right) \left(\frac{n-s+t}{2} + t\alpha_n \right)$$

ss i g n is e e t is s ca e si plified to

$$\beta_n = \frac{(2n+\ )2^n - (2n+\ )\binom{n}{n/}}{4} + \frac{(n+\ )2^n - (2n+\ )\binom{n}{n/}}{2}\ \alpha_n,$$

or if n is odd t e t e s eco es

$$\beta_n = \frac{(2n+\ )2^n - 4n\binom{n-}{(n-\ )/}}{4} + \frac{(n+\ )2^n - 4n\binom{n-}{(n-\ )/}}{2}\ \alpha_n.$$

Usi g eq atio 4 t is ea s t at if n is e e , t e

$$\alpha_n = \frac{(2n+\ )2^n - (2n+\ )\binom{n}{n/}}{(2n-2)2^n + (4n+2)\binom{n}{n/}}, \tag{5}$$

ilst if n is odd, t e

$$\alpha_n = \frac{(2n+\ )2^n - 4n\binom{n-}{(n-\ )/}}{(2n-2)2^n +\ n\binom{n-}{(n-\ )/}}. \tag{6}$$

it er a , si g tirli g's for la $n!$ $\overline{2\pi n} n^n e^{-n}$ e get t at

$$\binom{2k}{k} = \frac{(2k)!}{(k!)} \quad \frac{}{\overline{\pi k}} 2^{\ k} \quad 2^{\ k}$$

as k , a d t e e a e t at α_n as n .

I pr i t ct c rit f i t- ir i t r c s

ilvio icali a d eo id e i ⋆

IT ab a f e Sc e ce, a b dge, , US

e de c b e ac ec a a f d g a g a e :
e f a d a e e h d f c c g a -Sha - e g- a e che e ha e d be e e ac ec ha he g a a -Sha e h d a d
e e e d e ac ec a a *s -s ri n sis* b h g ha d g a g a e che e h e ec a be efe ab e f ea ab e ea e f c

I tr cti

. ct curit f i tur c s

old asser, icali a d ivest's ([ ]) classical otio of securit for a digital sig ature sche e is as ptotic i ature. I esse ce, a proof of securit a ou ts to a reductio fro forgi g a sig ature to solvi g a co putatio all hard pro le : if a pol o ial-ti e forger e ists, the e ca use it to solve the hard pro le i pol o ial ti e.

It has ee ofte poi ted out that this as ptotic approach, hich uses oti- o s such as "pol o ial ti e" a d "sufficie tl large," is too coarse for practical securit reco e datio s. K o i g that o pol o ial-ti e adversar has a etter tha e po e tiall s all cha ce of forger for a sufficie tl large securit para eter does ot provide o e ith a a s er to the practical pro le of fi - di g the appropriate securit para eters to e sure securit agai st adversaries ith certai co crete capa ilities.

ellare a d oga a ([96]) argue that, i order to e a le to deduce co crete securit reco e datio s, it is i porta t to e precise i the reductio fro a forger to the algorith that solves the hard pro le . or e a ple, if o e k o s that factori g i tegers of le gth is o ore tha ti es harder tha reaki g a certai sig ature sche e ith securit para eter , the o e could pick so that eve % of the ork required to factor i tegers of le gth is co sidered i feasi le.

⋆ f e f he a e a a ab e f `http://theory.lcs.mit.edu/~reyzin/` The ec d a h a ed a de a a a Sc e ce da ad a e e h

. au gar (d.): ' , 7 , pp. 7– , .

reductio i hich the difficult of forgi g a d the difficult of solvi g the u derl i g hard pro le are close is called *t ht*; other ise, it is called *s* . (aturall , "close," "tight" a d "loose" are i precise ter s a d ake ore se se he used i the co parative.) sche e hose e act securit is tightl related to the difficult of factori g is also proposed i [96].

. s curit f i t- ir- ik i tur c s

fruitful ethod for co structi g sig ature sche es as i troduced iat a d ha ir ([6]). lthough clai ed for a specific I sche e, the ethod orks ith a ge eral *c mm t cha r s* I sche e. he ethod co sists of replaci g the verifier's ra do challe ge a pu licl k o "ra do " fu ctio co puted o the prover's co it e t a d the essage ei g sig ed. his re oves i teractio a d adds the essage i to the picture, thus cha gi g a I sche e i to a sig ature sche e.

a of such sig ature sche es have ee prove secure he the "ra do " fu ctio is odeled as a ra do oracle ([93] provide a for al treat e t of this odel). Ho ever, the reductio s i these proofs are quite loose, thus ecessitati g larger ke si es. U less a tighter reductio has ee overlooked, the o l a to i prove the securit of such sig ature sche es is to odif the to allo for tighter reductio s.

.3 tri uti s f t is p r

his paper akes t o co tri utio s.

irst, e sho ho to odif the factori g- ased iat- ha ir-like sche es to akes their securit ver tightl related to the pro le of i teger factori a-tio . ur odificatio is quite ge eral a d ca e applied, i particular, to the sche es fro [6], [ ], [ ], [ ], [9], [ka92], [ic94], [ho96] a d [ch96].

o e e plif our ethod a d ake the descriptio co crete, e picked o e of the si pler a d ore efficie t sche es fro the a ove list, the o e of [ic94]. s it is o l a *am* of a sche e that our ethod applies to, e shall he ceforth call it the " " sche e. e first prese t a e act a al sis of the loose securit of , the propose the odificatio (called the "s ap ethod") a d prese t a e act a al sis of the tight securit of the odified sche e (called " -s ap").

ote that oth a d -s ap are quite practical, ith the perfor a ce that is co para le to that of the sche es curre tl used i practice.

eco d, after proposi g a ethod for creati g sig ature sche es ith tight reductio s, e de o strate that tight ess of a reductio alo e is i sufficie t if o e ishes to a i i e securit hile i i i i g costs other tha ke le gth (e.g., sig i g ti e). hile it is i deed true that a tighter reductio allo s for a lo er securit para eter, a "loose" sche e ca e so efficie t that, though requiri g a larger securit para eter for a *s c fi f s c r t* , a deliver etter perfor a ce (e.g., i sig i g ti e) tha a "tight" sche e for the sa e level of securit .

pecificall , e de o strate that although -s ap has etter e act securit tha the sche e, hich of the t o sche es to pick depe ds o hat the ai factor i the cost is. If the efficie c of verif i g is of ai co cer , the -s ap should e chose . If, ho ever, the efficie c of sig i g is the ai co cer , the the sche e ca deliver ore securit for less cost. I fact, i that case the sche e ca deliver ore securit for less cost tha eve the sche es of [96].

e highlight that our poi t is ot sacrifici g securit for efficie c . uite co trar , e leverage efficie c i order to achieve etter securit . e su it that easuri g the cost of a sig ature sche e accuratel is just as i porta t as easuri g securit accuratel , a d de o strate that sche es ith orse e act securit a actuall achieve etter securit for the sa e cost. e hope that this a further the applica ilit of e act securit a al sis.

.4 p

e egi i troduci g for al defi itio s a d deali g ith other preli i aries i ectio 2. e i troduce the sig ature sche e a d a al e its securit i ectio 3. ur e ethod for co structi g sig ature sche es is give i ectio 4. e the sho i ectio 5 ho to appl e act securit a al sis to choosi g a digital sig ature sche e so as to opti i e a give cost for a give level of securit .

iti s

I the i terests of space, e o it the e pla atio s of co o l used otatio a d the ofte -used defi itio of a sig ature sche e as a triple of algorith s that are give access to a co o oracle (see, e.g., [93] a d [96]). he are availa le i the full paper.

e ill, ho ever, provide a ore detailed discussio of hat it ea s for a sig ature sche e to e secure. ur defi itio of securit is a odified versio of that i [96], hich is ased o [93] a d [ ]. his defi itio co cer s itself ith e act, rather tha as ptotic, securit .

I tuitivel , e a t to capture the follo i g i our defi itio of securit : there is o algorith (called “forger”) that, for a ra do oracle , is a le to produce e valid sig atures ith reaso a le pro a ilit i reaso a le ti e ithout k o i g the secret ke *sk*. oreover, e should assu e that a attacker ca coerce the sig er i to sig i g so e u er of essages of the attacker’s choice—to carr out the so-called “adaptive chose - essage attack” [ ]. e odel this givi g the forger oracle access to the oracle a d to the algorith $^{H}(sk \ \cdot)$.

iti . forger ’ *s a r a st c t rac a r thm that s a s c r t aram t r k a a c pk as t. h first rac f s ca a* hashi g oracle *a th s c rac s ca a* sig ature oracle*. t a hash rac a t* $(pk \ sk) = \ ^{H}(\ ^{k})$ *f r s m k. sa that th*

f r r succeeds *f* ( ) $^{H,Sign^H(sk,\cdot)}($ ^{k} *pk*) *a s a a s at r a t q r ts s at r rac* .

sa that a f r r (*t* $_{sig}$ $_{hash}$) *r a s th s at r sch m f f r a s c r t aram t r k th f h s*

- *ts r t m* (*s th s f ts scr t*) *s t c* *t*(*k*)
- *th m r f ts q r s t th s at r rac s t c* $_{sig}(k)$
- *th m r f ts q r s t th hash rac s t c* $_{hash}(k)$
- *th r a t at ast* (*k*) $^H($ $^k)$ *rat s s ch a* (*pk sk*) *that th r a t f th f r r's s cc ss t* (^{k} *pk*) *s at ast* (*k*) *(h r th r a t f th f r r's s cc ss s ta r a ra m ch c f th rac th ra m ta f th f r r th ra m ta f th s r t h m th f r r a r ss s th ch s m ssa q r s t t th ch c f pk)*

a sa that a s at r sch m s (*t* $_{sig}$ $_{hash}$) *s c r f f r r* (*t* $_{sig}$ $_{hash}$) *r a s t.*

(s a aside for the reader fa iliar ith the defi itio of [96], e poi t out that if a sche e is (*t* $_{sig}$ $_{hash}$)-secure i the se se of the [96], the it is (*t* $_{sig}$ $_{hash}$)-secure i the se se of the a ove defi itio . e si pl separate the co po e t of the pro a ilit that is due to the selectio of the pu lic ke .)

o that e have defi ed hat it ea s for a sig ature sche e to e secure, ho do e actuall prove a thi g a out securit ? e ill relate the securit of a sig ature sche e to the difficult of so e pro le ; i our case, the difficult of factori g. et (^{l}) e a algorith ge erati g - it products of t o pri es.

iti . *sa that a a r thm* (*t*) *fact rs t rs ra t f f r a aram t r*

- *'s r t m* (*s th s f ts scr t*) *s t c* *t*( )
- *th r a t at ast* ( ) (^{l}) *rat s s ch a t r that has at ast* ( ) *r a t (ta r th ra m ch c s f th a r thm t th ch c f) f r c th c rr ct fact rs f t*

sa that fact r t rs rat s (*t*) *s c r f s ch sts.*

ive this defi itio of the difficult of a pro le , e ca the e plai the securit of a sig ature sche e i the follo i g ter s, as suggested [96]: if so e pro le is (*t*)-secure, the sche e is (*t* $_{sig}$ $_{hash}$)-secure. If *t* is ot uch s aller tha *t* a d are ot uch larger tha , , eve for a reaso a l large $_{sig}$ a d $_{hash}$, the the reductio provi g the securit is called *t ht.*

3 c

3. i tur ri c ti rit s

e descri e the follo i g I a d sig ature sche e fro [ic94], ith si ilarities to the g- ch orr ([9]) a d the uillou- uisquater ([ ]) sche es.

NUMBER THEORY. et k a d e t o securit para eters. et p 3 (od) a d p 7 (od) e t o pri es of appro i atel equal si e a d $= p\ p$ e a - it i teger (such is called a *ams* i teger [il]). o si plif further co putatio s, e ill assu e ot o l that 2^{l-} , ut also that $_n$ = $- p$ $- p$ + 2^{l-} , a d that p + p − $2^{l/}$. et de ote the set of o - ero quadratic residues odulo . ote that 2^{l-} . ote also that for , e actl o e of its four square roots is also i (this follo s fro the fact that − is a o -square odulo p a d p a d the hi ese re ai der theore). hus, squari g is a per utatio over . ro o o , he e speak of "the square root of ," e ea the si gle square root i ; $^{-k}$ e ill de ote the si gle such that = ^{k}. lso ote that 2 is a o -square odulo p a d a square odulo p (ecause $\frac{}{p}$ = (− $)^{(p\ -\ )/}$), so a d − 2 −2 . I ge eral, for a $_n$, e actl o e of − 2 −2 is i .

ollo i g [ ], defi e ( ) = od , ( ) = 4 od , a d, for a m- it i ar stri g σ = . . . $_m$, defi e $_\sigma$: as $_\sigma$( ) = $_{b_m}$(. . . ($_b$ ($_b$ ( ))) . . .) = ^{m} 4^σ od (ote that 4^σ is a slight a use of otatio , ecause σ is a i ar stri g, rather tha a i teger; hat is reall ea t here is 4 raised to the po er of the i teger represe ted i i ar σ). ecause squari g is a per utatio over a d 4 , $_\sigma$ is a per utatio over .

ote that $_\sigma$( ) ca e efficie tl co puted a od ho k o s . lso, if o e k o s p a d p , o e ca efficie tl co pute = $\bar{}_\sigma$ ( ) (as sho oldreich i [ol 6]) co puti g s = 4 $^{-\sigma}$ od a d the letti g = $^{-\sigma}$ s^σ od (these calculatio s ca e do e odulo p a d p separatel , a d the results co i ed usi g the hi ese re ai der theore). Ho ever, if o e does ot k o p a d p , the $\bar{}_\sigma$ is hard to co pute, as sho i the e a elo .

. *If ca c m t f r a a t ff r t str s* σ *a* τ *f q a th* = $\bar{}_\sigma$ ( ) *a* = $\bar{}_\tau$ ( ) *th ca fact r* .

r f. he proof is i ductio o the le gth of the stri gs σ a d τ.

If σ = τ = , the assu e, ithout loss of ge eralit , that σ = a d τ = . he ( ) ( ) od , i.e., 4 od , i.e., (− 2)(+ 2). ote that a d 2 , so 2 , so 2 (od), so does ot divide either − 2 or + 2 . hus, co puti g the gcd of + 2 a d , e ca get either p or p .

or the i ductive case, let σ a d τ e t o stri gs of le gth $m+$. et σ a d τ e their m- it prefi es, respectivel . If $_\sigma$ ( ) $_\tau$ ( ) (od), e are do e the i ductive h pothesis. ther ise, the last it of σ ust e differe t

fro the last it of τ, so, ithout loss of ge eralit , assu e the last it of σ is a d the last it of τ is . he ($_\sigma$ ( ) ($_\tau$ ( ) (od), a d the sa e proof as for the ase case orks here.

THE ID SCHEME. he a ove le a aturall suggests the follo i g I sche e. user has as the pu lic ke a d p p as the secret ke . o prove his ide tit (i.e., that he k o s p a d p) to a verifier, he co its to ra do X a d se ds it to the verifier. he verifier produces a ra do k- it challe ge σ a d se ds it to the prover (the user). he prover respo ds ith $=$ $\bar{}_\sigma\,(X)$ (ote that σ here is prefi ed ith a si gle it, hose use ill e e plai ed shortl). he verifier checks that $X =$ $_\sigma$( ) $=$ $_\sigma$( ) a d that (od). I for all , the securit of this protocol is ased o the fact that if the prover is a le to respo d to t o differe t challe ges σ a d τ, the , e a , he k o s p a d p . he it i fro t of σ is to save the verifier fro havi g to check that the prover's respo se is i (hich is a hard pro le i itself)—i stead, she just squares the prover's respo se a d thus puts it i .

e ill sa o ore a out the securit of this I sche e ecause e are ot co cer ed ith it i this paper. e ill, ho ever, poi t out a efficie c i prove e t for the prover. irst, as part of ke ge eratio , the prover co - putes, usi g the hi ese re ai der theore , $s =$ 4 $^{-k-}$ od . he , he co itti g to a ra do X , the prover ra do l selects a $_n$ a d sets $X =$ ^{k} od (ote that X gets selected ith u ifor distri utio as lo g as is so selected). o , to respo d to a challe ge σ, the prover si pl co putes $=$ s^σ od .

THE E SCHEME. he sta dard a to cha ge the a ove I sche e i to a sig ature sche e is to replace the verifier ith a ra do fu ctio : } }^{k}. he e act steps of the algorith s , a d follo .

Ke e eratio

. e erate t o ra do pri es p 3 (od) a d p 7 (od) a d $= p\ p$ so that 2^l, $-p$ $-p$ $+$ $2^l +$ a d p $+p$ $-$ $2^{l/}$

2. e erate coefficie t $= p$ $^-$ od p for use i the hi ese re ai der theore

3. o pute $u_i = \big(\frac{p_i}{\ }$ ^{k} od $\frac{p_i-}{\ }$ for $=$ 2 (ote that u_i is such that raisi g a square to the po er u_i odulo p_i ill co pute its 2^k root)

4. o pute $s_i = \big(\frac{p_i}{\ }$ ^{u_i} od p_i for $=$ 2

5. o pute $v = (s\ -s\ )$ od p a d $s = s\ + vp$ to get $s =$ 4 $^{-\ k}$ od

6. utput as the pu lic ke a d (s) as the secret ke

ig i g

. e erate X picki g a ra do $_n$ a d co puti g $X =$ ^{k} od (ote that this step ca e do e off-li e, efore the essage is k o)

2. o pute $\sigma =$ (X), a d $=$ $\bar{}_\sigma\,(X)$ via $t = s^\sigma$ od (this ca e do e via $t_i = s_i^\sigma$ od p_i for $=$ 2, $v = (t\ -t\ )$ od p , $t = t\ + vp$) a d $=$ t od

3. utput (σ)

erif i g

. erif that (od) a d co pute $X = {}_{\sigma}(\ )$ via $t = {}^{k}$ od , $t = 2^{\sigma}$ od , $X = t\ t$ od

2. erif if $\sigma = (X\ )$

3. curit f t sc

e state the follo i g t o theore s that give t o differe t vie s of the e act securit of the sche e a d de o strate the tradeoff et ee ru i g ti e a d success pro a ilit . heir proofs use k o ethods (see oi tcheval a d ter [96] a d hta a d ka oto [9]). ur pro a ilit a al sis is e , ho ever, a d results i slightl tighter reductio s.

r . *If th r sts a f r r that* $(t\ {}_{sig}\ {}_{hash}\ )$ *r a s th sch m th s c r t aram t rs a k th th r sts a a r thm that* $(t\ )$ *fact rs t rs rat f r*

$$t = 2t + 2(\ {}_{sig} +\ )T + T$$

$$= \frac{}{{}_{hash} +} - 2^{-k}\ (\ - 2\gamma)$$

h r T *s th t m r q r t rf rm a s at r r ficat* T *s th t m r q r t fact r th c t s f mma (ss t a a c c m tat) a* $\gamma = {}_{sig}(\ {}_{hash} +\ )2^{-l}$ *(t that* γ *s c s t f r a ar h).*

r f. et e a forger that $(t\ {}_{sig}\ {}_{hash}\ )$- reaks sig ature sche e. e ill co struct a factori g algorith that uses to produce ${}_{n}$ a d $\sigma = \tau\ \}^{k}$ such that ${}_{\sigma}(\ ) = {}_{\tau}(\ )$. his ill allo to factor usi g the ethod give i the proof of e a .

he ai idea of this proof is give the "forki g le a" of [96]. It is to allo to ru o ce to produce o e forger —a sig ature (σ) o a essage such that $\sigma = (X\ )$ here $X = {}_{\sigma}(\ )$. ote that had to ask a hashi g-oracle quer o $(X\ )$—other ise its pro a ilit of success is at ost 2^{-k}. he , ru the seco d ti e, givi g the sa e a s ers to all the oracle queries efore the quer $(X\ )$. or $(X\ )$ give a e a s er τ. he , if agai forges a sig ature (τ) usi g X a d , e ill have achieved our goal.

ssu i g is such that has pro a ilit at least of success, the pro a ilit that ill factor usi g this approach is roughl ${}_{hash}$, ecause eeds to succeed t ice a d e have o guara tee that ill choose to use $(X\ )$ for its seco d forger a d ot a of its other ${}_{hash}$ oracle queries.

he co plete details of the proof are availa le i the full versio of this paper a d are o itted here i the i terests of space.

r . *If th r sts a f r r that* $(t\ {}_{sig}\ {}_{hash}\ )$ *r a s th sch m th s c r t aram t rs a k s ch that* $2^{-k}\ (\ {}_{hash} +\ )\ (\ -\ {}_{sig}(\ {}_{hash} +$

$)2^{-l}$ $)$ *th th r sts a a r thm that* $(t$ $)$ *fact rs t rs rat f r*

$$t = \frac{(2 \ _{hash} + 3)(t + \ _{sig} T \ )}{(\ - \gamma) - 2^{-k} \ \ (\ _{hash} + \ )} + T$$

$$= \frac{}{2} \quad - - \quad . \ 99$$

h r T T *a* γ *ar as h r m .*

r f. he idea is to iterate the fro heore sufficie tl a ti es to get a co sta t pro a ilit of success. ore specificall , ru a out ti es the first ti e, to achieve a co sta t pro a ilit of a successful forger , a d a out $2 \ _{hash}$ ti es the seco d ti e, to achieve a co sta t pro a ilit of a successful forger that uses the pair $(X$ $)$.

he co plete details of the proof are availa le i the full versio of this paper a d are o itted here i the i terests of space.

he follo i g t o state e ts follo directl fro the theore s just proved o ce e fi the para eters to e high e ough to avoid deali g ith s all ter s.

r r . *If fact r t t rs rat s* $(t$ $)$ *s c r th th s at r sch m s* $(t \ _{sig} \ _{hash}$ $)$ *s c r f r*

$$_{sig} \quad 2^{l-} \quad (\ _{hash} + \ )$$

$$t = t \quad 2 - (\ _{sig} + \ )T \ \ - T \quad 2$$

$$= 2^{-k}(\ _{hash} + \ ) + \quad \overline{2 \ \ (\ _{hash} + \ )}$$

r f. ote that the value for t follo s directl solvi g for t the equatio for t i the state e t of heore . he value for is co puted as follo s: solve for the quadratic equatio that e presses i ter s of to get

$$= \quad 2^{-k}(\ _{hash} + \ ) + \quad \overline{2^{- \ k}(\ _{hash} + \ ) \ + 4 \ \ (\ _{hash} + \ ) \ (\ \ - 2\gamma)} \quad 2$$

$$2^{-k}(\ _{hash} + \ ) + \quad \overline{2^{- \ k}(\ _{hash} + \ )} \ + \quad \overline{4 \ \ (\ _{hash} + \ ) \ (\ \ - 2\gamma)} \quad 2$$

$$= 2^{-k}(\ _{hash} + \ ) + \quad \overline{(\ _{hash} + \ ) \ (\ \ - 2\gamma)}.$$

serve that e are allo ed to i crease , as this ill o l eake the result. ote that the co ditio o $_{sig}$ e sures that $- 2\gamma$ 2, so setti g to $2^{-k}(\ _{hash} + \ ) + \ \overline{2 \ \ (\ _{hash} + \ )}$ ill ot decrease it.

r r . *If fact r t t rs rat s* $(t$ $. \ 99$ $)$ *s c r th th s at r sch m s* $(t \ _{sig} \ _{hash}$ $)$ *s c r f r*

$$t = \frac{(t \ \ - T \ )}{4 \ _{hash} + 6} - \ _{sig} T$$

as *as*

$$
\begin{aligned}
{}_{sig} \quad & 2^{l-} \quad ({}_{hash} + \quad) \\
& 2^{-k} \quad ({}_{hash} + \quad).
\end{aligned}
$$

r f. he proof is si ilar to that of of orollar , a d is give i the full paper.

4 p t

4. ti ti

s e e plified the proof of heore s a d 2 a ove, all k o results for the securit of iat- ha ir-like sig ature sche es i volve losi g a factor of ${}_{hash}$ (i either ti e or success pro a ilit) i the reductio fro a forger to a algorith that reaks the u derl i g hard pro le (see, for e a ple, [6], [ch96], [96], [ho96], [9]). hile o proof e ists that the loss of this factor is ecessar , the pro le see s i here t i the a sig ature sche es are co structed fro I sche es, as e plai ed elo .

he securit of a I sche e usuall relies o the fact that a prover ould e u a le to a s er t o differe t challe ges for the sa e co it e t ithout k o i g the private ke . herefore, i the proof of securit of the correspo di g sig ature sche e, e eed to use the forger to get t o sig atures o the sa e co it e t, as e did i the proof of heore s a d 2. he forger, ho ever, has a of its ${}_{hash}$ queries to pick for the co it e t for the seco d sig ature—he ce, our loss of the factor of ${}_{hash}$. e a t to poi t out that ${}_{hash}$ is a sig ifica t factor, a d its loss defi itel akes a reductio quite loose. his is ecause a reaso a le ou d o the u er of possi le hash queries of co itted adversaries is a out ${}_{hash} = 2$ (see ectio 4.4).

e therefore devise a e ethod of co structi g sig ature sche es fro I sche es so that a o e sig ature fro the forger is e ough to reak the u derl i g hard pro le .

4. t

ecall that i iat- ha ir-like sig ature sche es, the sig er co es up ith the co it e t a d the uses applied to the co it e t a d the essage to produce the challe ge. e propose that i stead the sig er *first c m th th cha a th s a t th cha a th m ssa t r c th c mm tm t.* I a a , e s ap the challe ge a d the co it e t.

his ethod applies he ever the sig er ca co pute the respo se give o l the challe ge a d the co it e t. It does ot appl he i for atio used duri g the ge eratio of the co it e t is ecessar to co pute the respo se. or e a ple, it does ot appl to discrete-logarith - ased I sche es (such as the ch orr sche e [ch 9]) i hich the prover eeds to k o the discrete logarith of the co it e t i order to provide the respo se.

dditio all , i order to use this ethod, o e eeds to get arou d the pro- le that the co it e t is selected fro so e structured set (such as i the case of), hile retur s a ra do i ar stri g. his pro le ca usuall e easil solved. he o l case k o to us he it see s to prese t a real o stacle is i the sche e of hta a d ka oto ([ ]) i the case he a e po e t L is used such that gcd(L (p −)(p −)) 2.

he ke -ge eratio algorith a d the private ke a eed to e odified slightl i order to provide the sig er ith the additio al i for atio eeded to co pute the respo se fro a ra do co it e t, rather tha fro a co it- e t that it ge erated. he verificatio algorith re ai s vastl u cha ged.

I the e t sectio , e e e plif our proposed ethod a d e plai h it results a tighter securit reductio .

4.3 -s p

scripti . he sche e depe ds o t o securit para eters: k a d . et : } $\}^{l-}$ e a ra do fu ctio .

Ke e eratio he ke ge eratio is the sa e as i the sche e, e cept for o e additio al step (step 6) a d e tra i for atio i the private ke :

. e erate t o ra do pri es p 3 (od) a d p 7 (od) a d $= p\ p$ so that 2^l, $-p\ -p\ +$ $2^l +$ a d $p\ + p\ -$ $2^{l/}$
2. e erate coefficie t $= p^{-}$ od p for use i the hi ese re ai der theore
3. o pute $u_i = \big(\frac{p_i}{}\big)^{k}$ od $\frac{p_i -}{}$ for $=$ 2 (ote that u_i is such that raisi g a square to the po er u_i odulo p_i ill co pute its 2^k root)
4. o pute $s_i = \big(\frac{p_i}{}\big)^{u_i}$ od p_i for $=$ 2
5. o pute $v = (s\ - s\ )$ od p a d $s = s\ + vp$ to get $s =\ 4^{-\ k}$ od
6. If u_i is odd, ake it eve setti g $u_i = u_i + \frac{p_i -}{}$ for $=$ 2 (ote that o u_i is such that raisi g a square or its egative to the po er u_i odulo p_i ill co pute its 2^k root)
7. utput as the pu lic ke a d ($s\ u\ u\ p\ p$) as the secret ke

ig i g

. e erate a ra do σ a d co pute $t = s^{\sigma}$ od (ote that this step ca e do e off-li e, efore the essage is k o).
2. o pute $X =$ $(\sigma$). e ill assu e X $_n$ (i.e., (X) =), ecause the pro a ilit of X $_n$ is at ost $2^{-l/}$. If the aco i s ol $\big(\frac{X}{n}\big) = -$, set $X = 2X$ od . o either X or $-X$ is i . o pute $=$ σ^{-} (X) via $_i = X^{u_i}$ od p_i for $=$ 2, $v = ($ $-$ $)$ od p , $=$ $+vp$ a d $=$ t od .
3. utput (σ).

erif i g

. erif that (od) a d co pute $X =$ $_\sigma$( ) via t $=$ ^{k} od , t $= 2^{\sigma}$ od , $X = t\ t$ od (this step is the sa e as for the sche e).
2. et $X =$ $(\sigma$). If X X (od) or X $2X$ (od), accept the sig ature (this step differs slightl fro the sche e).

curit f -s p.

r 3. *If th r sts a f r r that* $(t \; {}_{sig} \; {}_{hash} \;)$ *r a s th s a sch m th s c r t aram t rs a k th th r sts a a r thm that* $(t \;)$ *fact rs t rs rat f r*

$$t \; = t + 2(\; {}_{sig} + \; {}_{hash} + \;)T \; + T$$
$$= \; (\; - \gamma) - (\; {}_{hash} + \; {}_{sig} + \;)2^{-l/}$$

h r T s th t m r q r t rf rm a s a s at r r ficat T s th t m r q r t fact r th c t s f mma (ss t a a c c m tat) a $\gamma = \; {}_{sig}(\; {}_{hash} + \;)2^{-k}$ *(t that* γ *s c s t f r a ar h k).*

r f. a iliarit ith the proof of heore ill e helpful for u dersta di g this proof.

et e a forger that $(t \; {}_{sig} \; {}_{hash} \;)$- reaks -s ap sig ature sche e. i ilarl to the proof of heore , e ill co struct a algorith that, after i teracti g ith , ill produce ${}_{n}$ a d $\sigma = \tau$ $\}^k$ such that ${}_{\sigma}(\;) = \; {}_{\tau}(\;)$.

he ai idea is to a s er each hash quer o $(\sigma \;)$ ith a X co puted via $X = \; {}_{\tau}(\;)$ for a ra do ${}_{n}$ a d ar itrar τ that is differe t fro σ. he if forges a sig ature $(\; \sigma)$ o , e ill have ${}_{\sigma}(\;) = \; {}_{\tau}(\;)$ a d ill e a le to factor .

he co plete details of the proof are availa le i the full versio of this paper a d are o itted here i the i terests of space.

r 4. *If th r sts a f r r that* $(t \; {}_{sig} \; {}_{hash} \;)$ *r a s th s a sch m th s c r t aram t rs a k s ch that*

$$(\; {}_{hash} + \; {}_{sig} + \;)2^{-l/} \qquad (\; - \; {}_{sig}(\; {}_{hash} + \;)2^{-k}$$

th th r sts a a r thm that $(t \;)$ *fact rs t rs rat f r*

$$t \; = \frac{t + 2(\; {}_{sig} + \; {}_{hash} + \;)T}{(\; - \gamma) - (\; {}_{hash} + \; {}_{sig} + \;)2^{-l/}} + T$$
$$= \; - - \; .632$$

h r T a T ar as h r m 3.

r f. et

$$= \; (\; - \gamma) - (\; {}_{hash} + \; {}_{sig} + \;)2^{-l/} \; .$$

assu ptio , . o if e repeat the algorith co structed i the proof of heore 3 up to ti es (e cept for the fi al gcd co putatio , hich eed o l e do e o ce), e ill get the desired , si ilarl to the proof of heore 2.

i ilarl to the sche e, e have the follo i g t o corollaries.

r r 3. *If fact r t t rs rat s (t) s c r th s a s at r sch m s (t $_{sig}$ $_{hash}$) s c r h r*

$$_{sig} \quad \mathrm{i}\ (2^{k-} \quad (\ _{hash} + \ ) \quad 2^{l/\ -} \ - \ _{hash} - \ )$$
$$t = t - 2(\ _{sig} + \ _{hash} + \ )T \ - T$$
$$= 2 \quad .$$

r f. he co ditio o $_{sig}$ e sures that $(\ -\gamma)-(\ _{hash}+\ _{sig}+\ )2^{-l}\ \ )$ 2. he rest follo s, si ilarl to the proof of orollar , fro solvi g the equatio s of heore 3 for t a d .

r r 4. *If fact r t t rs rat s (t .632) s c r th th s a s at r sch m s (t $_{sig}$ $_{hash}$) s c r f r*

$$_{sig} \quad \mathrm{i}\ (2^{k-} \quad (\ _{hash} + \ ) \quad 2^{l/\ -} \ - \ _{hash} - \ )$$
$$t = \frac{(t \ - T\ )}{2} - 2(\ _{sig} + \ _{hash} + \ )T \ .$$

r f. he co ditio o $_{sig}$ e sures that $(\ -\gamma)-(\ _{hash}+\ _{sig}+\ )2^{-l}\ \ )$ 2. he rest follo s, si ilarl to the proof of orollar 2, fro solvi g the equatio s of heore 4 for t a d .

4.4 r t r ic

he for ulas i the orollaries –4 are quite differe t. o etheless, it is i - ediatel clear that *s a s s fact r f* $_{hash}$ either i ti e or i pro a ilit . his is a ig adva tage for -s ap ecause $_{hash}$ ca e quite ig. fuller co pariso , provided i the e t sectio , depe ds o the actual values of the para eters $_{sig}$, $_{hash}$, k a d . et us deal here, ho ever, ith the preli i ar pro le of assig i g reaso a le values to these para eters.

e elieve it reaso a le to set $_{sig} = 2$ a d $_{hash} = 2\ \ -\ \ .$ his is so ecause sig ature queries have to e a s ered the ho est sig er (ho a ot e illi g or a le to sig ore tha a illio essages), hile hash queries ca e co puted the adversar alo e (ho a e illi g to i vest e traordi ar resources). otice that e reco e d a higher value for $_{hash}$ tha suggested i [96].

e reco e d setti g $k =$ for the sche e a d $k =$ 2 for -s ap. or the sche e, this is so ecause, fro orollaries a d 2, e see that $2^{-k}(\ _{hash} + \ )$ has to e s all (the value of $2^{-k}(\ _{hash} + \ )$ is esse tiall the success pro a ilit of the si ple attack that relies o correctl guessi g o e hash value a o g $_{hash} +$ hash queries). herefore, e eed 2^{-k} to e s all, a d setti g $k =$ e ake it less tha $^{-}$. or -s ap, this is so ecause 2^{k-} has to e at least $_{sig}(\ _{hash} + \ ) = 2$ fro orollaries 3 a d 4.

s for , otice that oth a d -s ap are i ediatel roke if the adversar succeeds i factori g the - it odulus. herefore, ought to e *at ast* . ive the a ove choices for the other para eters, such a i i u value for is large e ough to ake all the co strai ts i volvi g i orollaries –4 satisfied (for a reaso a le i the case of orollaries 3 a d 4). hus, the value of depe ds o the presu ed securit of factori g, as discussed i the e t sectio .

s f r ct c rit - st sis

. sts f curit

he desired level of securit is usuall dictated the specific applicatio . It is after settli g o the desired a ou t of securit that choosi g a o g the various secure sche es eco es crucial. I deed, he choosi g a sig ature sche e, the goal is *t ma ta th s r f s c r t at th st ss c st.* I a se se, picki g a sig ature sche e is si ilar to shoppi g for a i sura ce polic for the desired face value.

he costs of a sig ature sche e, ho ever, are quite varied. he a i clude the si es of ke s a d sig atures, the efficie cies of ge erati g ke s, sig i g a d verif i g, the a ou ts of code required, a d eve "e ter al" co sideratio s— such as the availa ilit of i e pe sive i ple e tatio s or off-the-shelf hard are co po e ts. I this paper, e focus o the efficie cies of sig i g a d verif i g. hese are particularl i porta t he sig i g or verif i g is perfor ed a lo -po er device, such as a s art card, or he sig i g or verif i g eeds to e perfor ed i ulk qua tities, as o a secure server.

It is for these costs, the , that elo e co pare the a d -s ap sche es. e also provide a co pariso of the sche e ith the a sche e fro [96], argua l the ost practical a o g those *t ht* related to factori g. (he reaso for choosi g a rather tha its varia t is that the latter is tightl related to , a d thus pote tiall less secure tha factori g.)

. p ris f -s p

he efficie c of sig ature verificatio i is a out the sa e as i -s ap. he securit of -s ap is ge erall higher tha the securit of for the sa e securit para eters. herefore, if the efficie c of verif i g is the o l sig ifica t co po e t i the cost, -s ap ill e a le to provide the sa e a ou t of securit for less cost tha .

ore difficult case to a al e is the case he the efficie c of sig i g is of ai co cer . e ill li it our a al sis to the case he e are o l co cer ed ith the o -li e part of sig i g. I oth cases, this i volves ai l a odular e po e tiatio . herefore, a variet of sophisticated alge raic ethods ca e used here, ut these ethods appl equall to a d -s ap. e thus fi d it si pler to co pare the t o u der "sta dard" i ple e tatio s usi g the hi ese

re ai der theore ( ). he the total a ou t of ti e required for o -li e sig i g i the sche e is a out $3k$ 4 a d the total required for o -li e sig i g i -s ap is a out 3 , ot cou ti g the (relativel s all) cost of co puti g the aco i s ol. (I su , o -li e sig i g is $(2k)$ ti es faster for tha for -s ap *f s th sam a f f r th.*)

et us o see ho the securit of the t o sche es co pares assu i g the o -li e sig i g costs are the sa e. et $_E$ a d k_E e the securit para eters for , a d $_{ES}$ a d k_{ES} e the securit para eters for -s ap. he o -li e sig i g costs for a d -s ap are the sa e if

$$_{ES} = (2k_E\ _E)^{\ /}\ . \qquad (\ )$$

he est k o factori g algorith s take ti e a out

$$T(\ ) = \quad e\ p \quad \frac{64}{9}^{\ /} \quad ^{\ /} (1 \quad)^{\ /}$$

for so e co sta t [93]. herefore, e ill assu e that factori g - it i -tegers ge erated is ($T(\ )$. 99)-secure for so e a d so e co -sta t . Usi g the for ulas give orollaries 2 a d 4 a d the values for $_{sig}$ $_{hash}$ k_E a d k_{ES} as give ectio 4.4, e ca o fi d out he the sche e eco es ore secure that -s ap if e keep the sig i g costs equal.

he details of further alge raic a ipulatio s are o itted here a d give i the full paper. he result is that at $_E = 6 \quad 9$, $_{ES} = \quad 954$, $k_E = \quad$, $k_{ES} = \quad 2$, a d -s ap provide a out the securit a d the sa e perfor a ce for o -li e sig i g. e o d this poi t, the gap i securit for the sa e perfor a ce i creases e po e tiall i favor of .

hus, the sig i g algorith of the sche e is so fast that prova le securit a d sig i g efficie c are the sa e he uses 6 9- it oduli a d -s ap 954- it oduli. I oth cases, the securit is that of factori g a 954- it i teger ge erated . (he sche e a actuall e eve ore secure, ut e ca ot prove it!)

It just so happe s that this co puted level of securit is curre tl co sidered adequate for a applicatio s. (herefore, for these applicatio s -s ap is prefera le: -s ap has faster verificatio for the sa e level of securit , as ell as shorter ke s a d, therefore, shorter sig atures.)

Ho ever, he ever the applicatio calls for a *h h r* level of securit , a d the do i a t cost is that of sig i g, the the "loosel "-secure eco es prefera le ecause the securit gap et ee a d -s ap, give the sa e perfor a ce, i creases e po e tiall .

---

e e , a a a a ab e E b E- a ec g e e f he fi ed ba e h e e add a e , e a e e e ed f he e f h a a

.3 p ris f t c it r - 's

he securit of a is tightl related to that of odular square roots, rather tha factori g. factor of 2 i pro a ilit is lost (as co pared to -s ap) he o e relates the securit of a to that of factori g. a 's perfor a ce for o -li e sig i g is a out the sa e as -s ap's (a requires a fe ore aco i s ol co putatio s, ut o separate odular ultiplicatio). vastl si ilar a al sis leads to the follo i g co clusio : prova le securit a d sig i g efficie c are the sa e he uses 59 9- it oduli, a d a 929- it oduli.

lso here this is a "cross-over" poi t: the gap i securit for the sa e performa ce i creases e po e tiall i favor of the sche e. s e ca see, this cross-over poi t is just slightl ore i favor of tha the cross-over poi t of a d -s ap. his is ecause of the factor of 2 differe ce i the securit of -s ap a d a .

c ts

e ould like to tha k alil adha for poi ti g out a error i a earlier versio of this ork a d ihir ellare for suggesti g a i prove e t i the securit a al sis of the sche e usi g a idea fro [99].

f r c s

h e a e a d Sa a e f a d- ec e d g a g a e che e I chae e e , ed , *dv n s in r g Y '* , e f r s in r i n S ge - e ag, 5 g Re ed e a a ab e f http://www.cs.ucsd.edu/ mihir/

R h e a e a d Ph R ga a Ra d ac e a e ac- ca : a ad g f de g g effic e c I *r - dings f h s nf r n n r nd - ni i n ri* , e be Re ed e a ea http://www-cse.ucsd.edu/users/mihir/papers/crypto-papers.html

R h e a e a d Ph R ga a The e ac ec f d g a g a e : g h RS a d Rab I a e [a], age 4 Re ed e a ea http://www-cse.ucsd.edu/users/mihir/papers/crypto-papers.html

Da I Da ga d, ed *dv n s in r g Y* , e 4 f *r s in r i n* S ge - e ag, , 4 a

S88 U e e ge, a , a d d Sha Ze - edge f f de *rn f r g* , : 4, 88

S8 a a d d Sha e e f: P ac ca de fica a d g a e b e I d [d 8], age 8 4

R88 Shafi d a e , S ca , a d R a d R e d g a g a e che e ec e aga ada e ch e - e age a ac *I rn n ing*, : 8 8, 88

PRab ha ff- e c e g g a d ha e effic e e fica

8 ded d e ch T e a c ce g he d a e- ca -R e g-
a e che e I d [d 8], age 4
88 S d a e , ed *dv n s in r g Y ’* , e 4
f *r s in r i n* S ge - e ag, , 5 g
88
Q88 a de a d ea - ac e Q a e a ad ca
de -ba ed g a e che e e g f e - edge I d-
a e [88], age
e a a d e a, ed *h d v n f h n r fi d*
si v , e 554 f *r n s in h i s* S ge - e ag,
a Ue a e , ed *dv n s in r g Y 6*, e
f *r s in r i n* S ge - e ag, a
c 4 S ca ec e a d effic e d g a g a e a g h Tech ca Re-
IT S T -5 , a ach e I e f Tech g , a b dge,
, a ch 4
S88 S ca a d d Sha e e f he a -Sha de fi-
ca a d g a e che e I d a e [88], age 44 4
d 8 d , ed *dv n s in r g Y ’ 6*, e
f *r s in r i n* S ge - e ag, 8 , 5 g
8
a Ta a a P ab ec e a d ac ca de fica che e a d
c e d g g a e che e I E e c e , ed , *dv n s*
in r g Y ’ , e 4 f *r s in r*
i n , age 5 S ge - e ag, , g
88 a h a a d Ta a a d fica f he a -Sha
che e I d a e [88], age 4
8 a h a a d Ta a a c c e e ec ea e f g-
a e de ed f de fica I g a c , ed , *dv n s*
in r g Y ’ , e 4 f *r s in r*
i n , age 54 S ge - e ag, g 8
S g a d P Sch a g a e ge e a h a a Sha - e
che e I Da ga d [Da], age 4 44
PS Da d P che a a d ac e S e Sec f f g a e che e
I a e [a], age 8 8
Q 8 - Q a e a d a de a e, ed *dv n s in r g*
Y , e 4 4 f *r s in r i n*
S ge - e ag, , 8
Sch8 P Sch Effic e de fica a d g a e f a ca d I
Q a e a d a de a e [Q 8], age 88 8
Sch P Sch Sec f ^{t}- de fica a d g a e I ea -
b , ed , *dv n s in r g Y ’ 6*, e f *r*
s in r i n , age 4 5 S ge - e ag, 8 g

Sh c Sh he ec f a ac ca de fica che e I a e
[a], age 44 5
8 gh a d fica f he RS b c- e e c ce-
d e *I r ns i ns n Inf r i n h r* , IT- : , e -
be 8

ri c I I t r t cc r ic i r r r

Y -Ya a

e a e f f a g ee g
h e e U e f g g
Sha g g
yychan8@ie.cuhk.edu.hk

he acce he e e a a e e e ce de SP f a e he a d h g acce he de a d h ch b ec e e gged he e e S ch da a e ab e e e hab be aced a d a a ed Th efe ed a c c a da a c ec a d a h ea e ac h a e e e ega a d ech ca f ec g e ac e e e ce a e d c ed e a e a c g a h c ha a a e e c ec a a SP h e he e de e ea ed he he he beha e h a e ca acce he e e a h e he a ca be ab ed

I tr cti

rapid d lopm t of t I t r t as mad a r ol tio o r o r dail lif . I formatio is ab da tl a d asil acc ssibl to r o o as a co ctio to t orld id i formatio s p r ig a . I t r t applicatio s lik l ctro- ic comm rc , l ctro ic m ssagi g (.g. -mails) as ll as t orld id b pro id gr at co i c to t mod r soci t a d t all tra sform comm rc , d catio , pro isio of go r m t s r ic s a d almost r ot r asp ct of mod r lif .

Ho r, t pri ac iss s accompa i g t s i o atio s ca ot b gl c- t d. pot tial i t rc ptio or mis s of p rso al data coll ct d from t pro isio of I t r t s r ic s is a t r at to s r pri ac . or o r, t rapid d lopm t of data mi i g t c ologi s mak s t is t r at mor s r . is r s lts i t calli g of a o mo s I t r t acc ss.

b li t at a o mit s o ld b pro id d co ditio all . I t lat r part of t is pap r, ill propos a cr ptograp ic sol tio t at ca ac i co ditio al a o mo s I t r t co ctio s, ic is d lop d bas d o t l ctro ic as rotocol i trod c d i [ ]. I o r protocol, s r a o mit is mai tai d so lo g as t s r do s ot misb a . I t is a , s r pri ac is prot ct d il a o mit is ot ab s d.

. au gar (d.): ' , 7 , pp. – , .

ri c I I t r t cc r ic

I t r t s r ic s pro id rs ca l ar m c abo t t ir c stom rs, as all i forma- tio t at ill pass to a I t r t s r m st rst pass t ro g t pro i s r sid i t ir s r rs. lt o g cr ptio t c iq s s c as ar s d so t at t ird parti s ca ot i t rpr t t co t ts b i g tra smitt d, t I ca still d t rmi at b sit s or ic articl a partic lar s r as isit d. is is b ca s r I t r t obj ct r q st origi at d from t s rs is logg d i t I 's pro cac . is is r f rr d as t 'clicktrails' data coll ctio . oll cti g a d a al i g t 'clicktrails' data ca d ri m c i formatio abo t a p rso .

. r s t ri c s o ici s

coll ctio of p rso al data is a oidabl i ma occasio s (.g. op i g a ba k acco t), om isti g pri ac ordi a c s s c as [2] allo s s r ic s pro id rs to coll ct s r's pri at i formatio for t p rpos i t d d, b t pr ts t m from c a gi g t sag of s c data. or t cas of I t r t s r ic s pro isio , at pr s t, a I as rig t to coll ct 'clicktrails' data a d old log l s of s r I t r t sag for t p rpos s of s st m mai t a c a d tro bl s ooti g. I di id al I also as o polic o pri ac , o r t sta dard di rg s a d s r pri ac is som tim s ot prop rl prot ct d.

. r s t o ous t r t r ic s o utio s

ral a o mo s I t r t s r ic s t c ologi s a b d lop d. aim at idi g t s r id tit from t r mot sit s. or ampl , t a o mo s b s r rs s c as [3] f tc s t r q st d obj cts o b alf of t s rs, so t at t r mot ost r c i s t r q st appar tl origi at d from t s r r. r ar also t c ologi s s c as t io o ti g [4] pro idi g a o mo s co ctio i ic ro ti g i formatio is idd .

. o itio o ous t r t cc ss r ic s

I ord r to pr t t ab s of t data i log l s, s rs s o ld r mai a o- mo s to t I d ri g I t r t obj ct r q sts. is ca b ac i d b si g cr ptograp ic m t ods. I ctio t r of t is pap r, ill pr s t a co ditio al a o mo s I t r t acc ss protocol t at a t follo i g f at r s:

- s r is a o mo s to t I d ri g I t r t acc ss.
- I as o a to r lat a r q st d obj ct to its r q st r if it is f tc d ia t I 's pro .
- a o mit is co ditio al, t s r id tit is r al d a misb - a ior is d t ct d.
- is protocol is tra spar t to ot r applicatio s; a d it is i t rop rabl amo g di r t I 's.

H r ass m t mplo m t of call r-I blocki g so t at t I ca ot trac t s r id tit from t p o mb r.

3 r t c

d lop d o r protocol moti at d b t - as protocol propos d i [2]. I o r s st m, t s r logi it a pass

$$(x, f(x)^{\ /} \pmod{n})$$

i ic t rst t rm is t ps do m of t s r a d t s co d t rm is t I 's p blic k sig at r [5]. H r is a p blis d composit a d o l t I k o s its factors, $f(.)$ is a o - a f ctio k o b bot t s r a d t I a d is t ps do m c os b t s r. rstl i trod c a simpl r rsio of t protocol, i ic a o mo s I t r t co ctio it o t s r id tit r co r is ac i d. I lat r s ctio , ill disc ss o t protocol is modi d so t at t s r's id tit ca b r al d i cas of a misb a ior occ rr c .

. ssu s ss to ic si g i ig tur 6] c

o op a acco t, lic g rat s a d , r is a ps do m ic s ill s to acc ss t I t r t s r ic s a d is a bli di g factor. s mb rs o l k o b lic . pr s ts t follo i g tok :

$$T = r \cdot f(x) \pmod{n}$$

to t I .

po r c i i g a d a i g ri d o lic 's id tit , t I sig s o b calc lati g t t ird root of mod lo a d r t r s $T^{\ /} \pmod{n}$, i. . $r \cdot f(x)^{\ /} \pmod{n}$, to lic . It is ass m d t at o l t s r r as t k o l dg to comp t t t ird root mod lo [5]. lic t tracts $f(x)^{\ /} \pmod{n}$ from t r t r d tok b di idi g $T^{\ /} \pmod{n}$ it a d form r pass:

$$pass = (x, f(x)^{\ /} \pmod{n}).$$

is pass is sa d at lic 's sid . logi s it t is a o mo s pass i st ad of r logi am from o o . s r r as o a to r lat lic to r ps do m b ca s it ca ot s t al of it sig s o t .

. ccou t p r tio s

acco t for is cr at d, r is t ps do m of lic . lic logi , s pr s ts t pass pass i st ad of si g r o s r am a d pass ord. t ticatio is do b rif i g t al of $f(x)^{\ /} \pmod{n}$. from pass. ll ot r acco t op ratio s ar similar to t isti g s st m. i c t s r r as o k o l dg o t id tit of , a o mo s I t r t s r ic pro isio is ac i d.

4 i r i it K cr r I tit

I ctio 3 a pr s t d t simpl r rsio of o r protocol. I t is s ctio , modif o it so t at t follo i g d sirabl additio al prop rti s ca b ac i d:

– lic is t o l l gitimat s r of t pass.
– lic 's id tit ill b r al d c ssar .

modi catio is bas d o t do bl sp di g pr tio sol tio pr - s t d i [2]. lat r prop rt abl s id tit r ocatio i critical sit atio s. I t modi d rsio of t protocol, a tr st t ird part ( ) is i ol d. d a alid pass as t follo i g format:

$$(pseudonym, \{pseudonym\}_{ISPsign}, \{pseudonym\}_{TTPsign}).$$

H r mak t sam ass mptio t at o l t I as t k o l dg to comp t t t ird root mod lo .

4. tti g ss

t a d b som t o-arg m t collisio -fr f ctio s as d scrib d i [2]. d l t b a iq id tif i g mb r of lic (.g. t acco t mb r). I st ad of prod ci g a si gl bli di g factor as i t pr io s s ctio , fo r i d p d t s ts of ra dom mb rs ac co sists of l m ts, , **c**, a d **r** ar g rat d.

I ord r to obtai t bli d sig at r from t I , lic forms a d s ds T_i's i t follo i g ma r:

$$T_i = r_i \cdot f(x_i, y_i) \pmod n$$

r

$$= \quad \text{to}$$
$$x_i = g(a_i, c_i)$$

a d

$$y_i = \quad (a_i \quad , d_i).$$

otic t at at t is stag , I k o s lic 's id tit , . I ord r to rif t T_i's pr s t d b lic , t I d rgo s t follo i g st ps:

. It c oos s ra doml a s t of /2 i t g rs, $R = \{i_j\}$, r $\leq i_j \leq k$ a d $\leq j \leq k/2$.
2. It asks lic to s o t al s of r_i, a_i, c_i a d d_i for r i .
3. It compar s t /2 pr s t d T_i's a d s if it is ca b d ri d from t s r_i, a_i, c_i, c_i a d .

ft r t at, t I gi s lic

$$\prod_{i \ R} T_i^{\ /} \pmod{n}$$

d lic ca asil tract t follo i g compo t:

$$\prod_{i \ R} f(x_i, y_i)^{\ /} \pmod{n}$$

ic is corr spo d to t I 's bli d sig at r o t ps do m,

$$p = \prod_{i \ R} f(x_i, y_i) \pmod{n}.$$

otic t at t I as o a to r lat to b ca s it ca ot s x_i a d y_i for $i \notin R$.

lic also ds to g t t sig at r from t . for sig i g o , t ri s t alidit of a d rit s part of t i formatio abo t lic 's id tit i to t databas . otic t at lic is a o mo s to t a d t i formatio obtai d b t is ot o g for it to comp t lic 's id tit .

o p rform t is task, t sam s t of T_i's ar pr s t d to t .

t p rforms t follo i g proc d r s:

. It asks lic to gi t al s of x_i, (a_i), a d d_i for r .
2. It ri s if t corr spo di g T_i's ca b d ri d from t pr s t d al s.
3. If t ri catio s cc ds, t stor s t al s (a_i) alo g it i to t databas .

t ri s a d sig s o t ps do m :

. or r $i \in R$ r $R = \{i \in \mathcal{Z} : i \notin R, \ \leq i_j \leq k\}$, it c cks if t al s of x_i, (a_i), a d d_i matc t corr spo di g T_i's i ol s i .
2. It sig s o t ps do m si g ormal p blic-k sig at r sc m s.

po r c i i g t 's sig at r , lic ca t form t pass:

$$(pseudonym, \{pseudonym\}_{ISPsign}, \{pseudonym\}_{TTPsign}).$$

I t proc ss of pass ri catio j st m tio d abo , t cr ptograp ic m t od, ro-k o l dg proof is mplo d. It abl s o to pro is/ r id - tit to t ot r part it o t r ali g t id tit . or d tails ca b fo d i [7].

4. ccou t p r tio s

cco t op ratio s ca b p rform d as s al. Ho r, t r ar som di - r c s i pass ri catio .

ri catio of a pass i cl d s t r proc d r s, am l t ri catio s of t I sig at r s a d t at of t sig at r s, a d also t proc ss to s r lic (o is a o mo s to t I) is i d d a alid old r of t pass. rst t o proc ss s ca b p rform d dir ctl si g t p blic-k sig- at r ri catio sc m s. il t last part is do b t follo i g:

. I g rat a ra dom bi ar ctor $Z = (z \; , z \; , ..., z_{k/} \;)$ r t l m t z_i corr spo d to t i^{th} mb r i t s t R .
2. lic r spo ds accordi g to t follo i g r l :
   - $z_i =$, lic s d t I a_i, c_i, a d y_i.
   - $z_i =$, lic s d t I x_i, a d y_i.
3. rom t r c i d al s, t I ca c ck if t corr spo di g T_i's ca satisf t pass.

4. tit oc tio

I t is protocol, a s r r mai s a o mo s so lo g as /s do s ot misb a . I t is a , a limit d a o mit is pro id d so t at s r pri ac ca ot b ab s d. is is do b t cr ptograp ic m t od of s cr t splitti g; i ic a pi c of s cr t is di id d amo g t o or mor parti s a d ac part alo do s ot a k o l dg abo t t s cr t [ ].

misb a ior of t old r of is d t ct d or i cas of a app als, t co rt asks t I to pr s ts t pass alo g it a_i for $i \in R$; ic it obtai s d ri g pass ri catio proc ss. co rt also gat rs t corr spo di g $(a_i$ $)$ for $j \in S$ r $S = R \cup R$ from t . otic t at $S \cup R \neq \{\emptyset\}$ a d l t b a l m t i $S \cup R$. s r id tit is r al d as:

$$u = a_e \qquad (a_e \qquad).$$

5 c rit i

is s ctio a al s o t str gt of o r protocol i r sista c of di r t pot tial t r ats.

. o it

lic r mai s a o mo s to t I . is is b ca s d ri g t stag of pass iss i g, lic pr par s ca didat s of T_i's a d t I o l ra dom c all g o /2 of t m. ot r /2 al s ic ar s d to form t pass ar r s b t I . ri g t a t ticatio proc ss, t I o l ra dom c all g o t /2 s al s. r for t I ca ot r lat t id tit of lic to t pass t at s poss ss s.

. squ r

ri g t pass iss i g stag , lic is ot a o mo s a d t I s o ld mak s r lic 's id tit b for sig i g o t pass. is ca b do b mplo i g a digital c rti cat sc m ; i ic o 's id tit is pro d b a r cog i d digital c rti cat . I t is a , t id tit of t pass r c i r ca b s r d.

. ic ts

i c t I i s o l alf of t ca didat s of r_i, a_i, c_i a d d_i, r $i \in R$, t r for i t pass iss i g proc ss lic ma a c a c to c at. do s t is b ot si g a alid i t calc latio of t os /2 T_i's ic ar ot i d b t I . Ho r r c a c of s cc ssf l c ati g d cr as po tiall it t al of . or ampl , q als 6, t c a c for t I c oosi g o of t lic 's c at d T_i's is /2 = . 39. i cr as s to 32 t c a c f rt r d cr as s to /2 6 = .526 × ⁻ .

.4 to ss

ppos lic 's pass is stol b arol d ri g t pass iss i g stag , t is ill ot bri g a lost to lic b ca s arol do s ot k o t s cr ts t at lic is oldi g. at is, arol do s ot k o a_i, c_i a d y_i for r $i \in R$ ic i ol i t ra dom c all g proc ss d ri g f t r logi s. r for ca ot s t pass.

ppos arol st als t pass at lat r stag s so t at s also st als t mb rs a_i, c_i a d y_i for som $i \in R$. I t is cas , o r, s ca ot s t pass til s obtai s a_i, c_i a d y_i for r $i \in R$. is is b ca s di r t l m ts i , c a d ar c all g d ra doml ac tim so arol ca o l obtai som of t m ac tim . arol as ait d lo g o g to coll ct a_i, c_i a d y_i for r $i \in R$, lic ma as alr ad c a g d r pass.

6 ci c

ompar it t o -a o mo s I t r t acc ss sc m , o r s c r a o mo s I t r t acc ss protocol ma r q ir mor comp tatio al po r. I t is s ctio a al o t comp tatio al ort i ol d.

6. o u r r tio

ri g t i itial stag r t pass is iss d, a total mb r of 4 ra dom i t g rs d to b g rat d. r is s itabl a d larg o g to pr t c at from a pot tial parti s, as plai d i ctio 5.3. or ampl , if = 32, t 2 ra dom mb rs ar g rat d.

mb r-of-bit of t s ra dom mb rs ar arbitrar . or ampl , 32-bit bi ar mb rs ar s d, t possibl ariatio for t al s of

r_i, a_i, c_i, d_i q als 2 = 4294967296. 64-bit bi ar mb r is s d i - st ad, t mb r of possibl ariatio s of t s al s is i cr as d to 2 = 446744 737 955 6 6. ig r t mb r-of-bit, t mor s c r b t slo- r of t s st m is.

6. ig i g o t ss.

i sig tur t . t I mak s a bli d sig at r o lic 's pass, it d to rif o t pass si g c t-a d-c oos m t od. is i ol s t ri catio o t /2 pr s t d T_i's; a d ac of t ri catio i ol s 3 as s. I also d to rif lic 's id tit a d t is i ol s o p blic- k c rti cat ri catio . r for t I ds to d rgo 3 /2 as s, o c rti cat ri catio a d p blic-k sig at r it sig s o a pass.

ig tur t . or t , t o proc d r s ar i ol d i t sig i g proc ss. irstl it ri s t x_i, (a_i), a d d_i for r . is i ol s 2 as s. co dl c cks if t /2 T_i's i ol s i t pass ar alid. is r q ir s a ot r as s. r for t ds to d rgo *3* as s a d p blic-k sig at r it sig o a pass.

6. ss i tio

a s r logi , t I d rgo s ra dom c all g a d c cks if t s r is a l gitimat old r of t pass. is i ol s a g ratio of a /2-bit ra dom bi ar mb r a d 2 as s, r is t mb r of 's i t bi ar mb r a d $z \in k/2$.

6.4 tit co r

t s r misb a s a d is/ r id tit is goi g to b r al d; t is simpl r q ir s o s arc i g a d o calc latio .

o co cl d , most op ratio s d rgo i o r protocol ar as s, a d t ar lig t i t rms of comp tatio al po r [9].

7 c i

I t is pap r a poi t d o t t pri ac probl ms i ol d i I t r t acc ss. also propos d a cr ptograp ic sol tio to t probl m; ic is mo- ti at d b t l ctro ic cas protocols. r protocol s pports a o mo s s r logi to a pro s r r so t at t I t r t sag abit of a s r ca ot b trac d a d a al d. Ho r t s r ca ot ab s is/ r a o mit b ca s o r protocol abl a misb a d s r's id tit to b r al d. is is ac i d b a k scro m t od i ic a tr st d t ird part k ps alf of t s cr t abo t t s r's id tit .

I additio , o r protocol r sid s o t applicatio la r a d do s ot r q ir c a g s i ot r la rs d ri g impl m tatio . it s itabl l gislatio , s r pri ac of I t r t acc ss ca b prop rl prot ct d.

ck t

a t or o ld lik to t a k rof ssor ictor . . i for is s p r isio o t r s arc .

r c

g g S R f he Pe e Re b c f h a: Pe a a a P ac d a ce e da e ec
a d ha a a : U aceab e ec c a h d a ce g P ceed g f RYPT 88 88
The e [eb age] h : a e c de h [cce ed Se]
4 Reed S e P d ch ag : P e f a g P ceed g h a e Sec ca fe e ce 5 4
5 R e R Sha a d d e a : e h d f b a g g a S g a e a d P b c e e ca f he 8
a d ha : d S g a e f U aceab e Pa e d a ce g P ceed g f RYPT 8 P e P e 8
ce Sch e e : ed g a h d d 4
8 e e : g a h c d g f a a a P ac R 8 Y e gh Y Re ea ch
ah Pe ce Te a : ec c Pa e S e

r p a al sis icr s s ica i si s (-)

r c c n i r , dg , and avid agn r

e a e S e
schneier@counterpane.com
h ea d ie
mudge@l0pht.com
U e ee
daw@cs.berkeley.edu

The P i - -P i T e i g P c PPTP i ed e- c e PPP c ec i e T P P i e e [S 8], ic - f e ea ed e e i he PPTP a he ica i echa i S- P , ca ed S- P e e e a e ie f he cha ge i he a he ica i a d e c i - e ge e a i i f S- P , a d a e he i e e a d e ai i g ea e e i ic f PPTP i e e a i

r d c i

oint-to- oint nn ling rotocol ( ) [H +97] is a protocol t at al- lo s oint-to- oint rotocol ( ) conn ctions [im94] to b t nn l d t ro g an I n t ork, cr ating a irt al rivat t ork ( ). icrosoft as impl - m nt d its o n algorit ms and protocols to s pport . is impl m ntation of , call d icrosoft , is s d t nsiv l in comm rcial pro- d cts pr cis l b ca s it is alr ad a part of t icrosoft indo s 95, 9 , and op rating s st ms.

a t ntication protocol in icrosoft is t icrosoft all ng / pl Hands ak rotocol (- H) [Z 9]; t ncr ption protocol is icrosoft oint to oint ncr ption ( ) [Z9]. ft r icrosoft's as cr ptanal d [9] and significant akn ss s r p blici d, icro- soft pgrad d t ir protocols [Zor9 a,Zor9 b,Zor99]. n v rsion is cal- l d - H v rsion 2 (- H v2); t old r v rsion as b n r nam d as - H v rsion (- H v). - H v2 is availabl as an pg- rad for icrosoft indo s 95, indo s 9 , and indo s 4. (.3) [ic9 a, ic9 b]. v n t o g t is pgrad is availabl , b li v t at most impl m ntation of s - H v .

is pap r amin s - H v2 and disc ss s o ll it addr ss s t s c rit akn ss s o tlin d in [9].

. au gar (d.): ' 7 pp. – .

most significant c ang s from - H v to - H v2 ar :

- ak r anag r as is no long r s nt along it t stron- g r indo s as . is is to pr v nt a tomatic pass ord crack rs lik p tcrack [99] from first br aking t ak r anag r as and t n sing t at information to br ak t strong r as [97].
- n a t ntication sc m for t s rv r as b n introd c d. is is to pr v nt malicio s s rv rs from masq rading as l gitimat s rv rs.
- c ang pass ord pack ts from - H v av b n r plac d b a singl c ang pass ord pack t in - H v2. is is to pr v nt t activ attack of spoofing - H fail r pack ts.
- s s niq k s in ac dir ction. is is to pr v nt t trivial cr ptanal tic attack of ing t t t str am in ac dir ction to r mov t ff cts of t ncr ption [9].

s c ang s do corr ct t major s c rit akn ss s of t original protocol: t incl sion of t anag r as f nction and t s of t sam ncr ption k m ltipl tim s. Ho v r, man s c rit probl ms ar still naddr ss d: .g., o t cli nt prot cts its lf, t fact t at t ncr ption k as t sam ntrop as t s r's pass ord, and t fact t at no g data is pass d on t ir to allo attack rs to mo nt cr pt-and-compar attacks. is b ing said, icrosoft obvio sl took t is opport nit to not onl fi som of t major cr ptograp ic akn ss s in t ir impl m ntation of , b t also to improv t q alit of t ir cod . n v rsion is m c mor rob st against d nial-of-s rvic st l attacks and no long r l aks information r garding t n mb r of activ s ssions.

- , rsi s a d

- H v c all ng /r spons m c anism as d scrib d in [9]. It consists of t follo ing st ps:

. li nt r q sts a login c all ng from t rv r.
2. rv r s nds back an -b t random c all ng .
3. li nt s s t anag r as of its pass ord to d riv t r k s. ac of t s k s is s d to ncr pt t c all ng . ll t r ncr pt d blocks ar concat nat d into a 24-b t r pl . li nt cr at s a s cond 24-b t r pl sing t indo s as and t sam proc d r .
4. s rv r s s t as s of t li nt's pass ord, stor d in a databas , to d cr pt t r pli s. If t d cr pt d blocks matc t c all ng , t a t- ntication compl t s and s nds a "s cc ss" pack t back to t cli nt.

is c ang as b n modifi d in - H v2. follo ing is t r vis d protocol:

. li nt r q sts a login c all ng from t rv r.
2. rv r s nds back a 6-b t random c all ng .

3a. li nt g n rat s a random 6-b t n mb r, call d t “ r t nti- cator all ng .”
3b. li nt g n rat s an -b t c all ng b as ing t 6-b t c all ng r c iv d in st p (2), t 6-b t r t nticator all ng g n rat d in st p (3a), and t li nt’s s rnam . (ction 3 for d tails.)
3c. li nt cr at s a 24-b t r pl , sing t indo s as f nction and t -b t c all ng g n rat d in st p (3b). is proc ss is id ntical to - H v .
3d. li nt s nds t rv r t r s lts of st ps (3a) and (3c).
4a. rv r s s t as s of t li nt’s pass ord, stor d in a databas , to d cr pt t r pli s. If t d cr pt d blocks matc t c all ng , t li nt is a t nticat d.
4b. rv r s s t 6-b t r t nticator all ng from t cli nt, as ll as t li nt’s as d pass ord, to cr at a 2 -b t “ t nticator spons .” (ction 5 for d tails.)
5. li nt also comp t s t t nticator spons . If t comp t d r - spons matc s t r c iv d r spons , t rv r is a t nticat d.

g n ral d scription of t c ang s b t n - H v and - H v2 is giv n in ig r . is protocol orks, and liminat s t most s rio s akn-

S- P e i	S- P e i
eg ia e P i h a a g i h a- e f 0x80	eg ia e P i h a a g i h a- e f 0x81
Se e e d a 8-b e cha e ge a e	Se e e d a -b e a e be ed b he c ie i c ea i g a 8-b e cha - e ge a e
ie e d 4-b e a d 4- b e T e e 8-b e cha e ge	ie e d -b e ee cha e ge ha a ed i c ea i g he hidde 8-b e cha e ge, a d he 4-b e T e e
Se e e d a e e a i g SU - SS UR	Se e e d a e e a i g SU - SS UR a d igg bac a he ica Re e he -b e ee cha e ge
ie decide c i e e d ba ed he SU SS UR e - e ab e	ie decide c i e e d ba- ed he SU SS UR e e ab e addi i , he ie chec he a idi f he he ica Re e a d di c ec if i i he e ec ed a e

S e ba ic diffe e ce be ee S P a d S P a he ica i

ss s t at plag d - H v . In - H v , t o parall l as val s r s nt from t li nt to t rv r: t anag r as and t indo s

as . s r t o diff r nt as s of t sam s r pass ord.
anag r as is a m c ak r as f nction, and pass ord-crack r programs s c as p tcrack r abl to br ak t anag r as and t n s t at information to br ak t indo s as [97]. liminating t a-nag r as in - H v2, icrosoft as mad t is divid -and-conq r attack impossibl . till, t s c rit of t is protocol is bas d on t pass ord s d, and p tcrack can still br ak ak pass ords sing a dictionar attack [99].

s ill disc ss lat r, m ltipl la rs of as ing ar s d in t diff r nt st ps of - H v2. il t is as ing s rv s to obsc r som of t val s, it is ncl ar at t cr ptograp ic significanc of t m ar . ll t s m to do is to slo do n t c tion of t protocol.

also av conc rns ov r t amo nt of control t cli nt as in t in-fl nc of t ltimat -b t c all ng t at is s d, t o g av not t b n abl to com p it a viabl attack to ploit t is. rtainl it op ns t possibilit of s bliminal c ann ls, ic can b ploit d in ot r cont ts.

3 - : ri i - all r 4- sp s

In - H v , t rv r s nds t li nt an -b t random c all ng . is c all ng is s d, tog t r it t li nt's pass ord and a as f nction, to cr at a pair of 24-b t r spons s.

In - H v2, t rv r s nds t li nt a 6-b t c all ng . is c al-l ng is not s d b t li nt dir ctl ; t li nt d riv s an -b t val from t is 6-b t c all ng . d rivation proc ss is as follo s:

. li nt cr at s a 6-b t random n mb r, call d t r t nticator all ng .
2. li nt concat nat s t r t nticator all ng it t 6-b t c all ng r c iv d from t s rv r and t li nt's s rnam .
3. cli nt as s t r s lt it H - [I 93].
4. first ig t b t s of t as b com t -b t c all ng .

It is t s b t s t at t li nt ill s to ncr pt t 6-b t local pass ord as (sing t indo s as f nction) to obtain t 24-b t r spons , ic t li nt ill s nd to t s rv r. is m t od is id ntical to - H v , and as b n d scrib d in [9].

. sis

It is ncl ar to s t is protocol is so complicat d. t first glanc , it s ms r asonabl t at t li nt not s t c all ng from t rv r dir ctl , sinc it is kno n to an av sdropp r. t inst ad of d riving a n c all ng from som s cr t information—t pass ord as , for ampl —t li nt s s a niq random n mb r t at is s nt to t rv r lat r in t protocol. r is no r ason t li nt cannot s t rv r's c all ng dir ctl and not s t r t nticator all ng at all.

4 - : ri i 4- sp s

ot - H v and - H v2 s t sam proc d r to d riv a 24-b t r spons from t -b t c all ng and t 6-b t pass ord as :

. 6-b t as is padd d to 2 b t s b app nding fiv ro b t s.
2. t X, Y, Z b t t r cons c tiv 7-b t blocks of t is 2 -b t val , and l t C b t -b t c all ng . 24-b t r spons R is calc lat d as $R = \langle \ {}_X(C), \ {}_Y(C), \ {}_Z(C)\rangle$.

4. sis

is complicat d proc d r cr at s a s rio s akn ss in t - H protocols: it allo s t attack r to sp d p dictionar k s arc b a factor of 2 , ic is a pr tt d vastating ff ct giv n t r lativ l lo ntrop of most s r pass ords.

ppos t at av sdrop on a - H conn ction. r spons R is pos d in t cl ar, and t c all ng C ma b d riv d asil from p blic information. ill att mpt to r cov r t pass ord, sing t kno l dg t at man pass ords ar clos l d riv d from dictionar ords or ot r is r adil g ssabl .

ot first t at t val of Z can b asil r cov r d: sinc t r ar onl 2 possibiliti s for Z, and av a kno n plaint t-cip rt t pair C, ${}_Z(C)$ for Z, ma tr ac of t possibiliti s for Z in t rn it a simpl trial ncr ption . is disclos s t last t o b t s of t as of t pass ord.

ill s t is obs rvation to sp d p dictionar s arc . In a on -tim pr comp tation, as ac of o r g ss s at t pass ord (p r aps as minor variations on a list of ords in a dictionar). sort t r s lts b t last t o b t s of t ir as and b rn t is on a - (or a small ard driv). n, n s a - H c ang , ma r cov r t last t o b t s of t as (sing t m t od o tlin d abov) and amin all t corr sponding ntri s on t - . is giv s s a list of pla sibl pass ords ic av t rig t val for t last t o b t s of t ir as ; t n can tr ac of t os possibiliti s b br t forc .

ppos a naiv dictionar attack o ld s arc N pass ords. In o r attack, tr onl t pass ords ic av t rig t val for t last t o b t s of t ir as , so p ct to tr onl abo t $N/2$ pass ords. is impli s t at t optimi d attack r ns abo t 2 tim s fast r t an a standard dictionar attack, if can afford t spac to stor a pr comp t d list of possibl pass ords.

is attack is applicabl to bot - H v and - H v2. Ho v r, t akn ss is m c mor important for - H v2, b ca s for - H v it is asi r to attack t an anag r as t an to attack t as .

is is a s rio s akn ss ic co ld av b n asil avoid d m r l b sing a standard cr ptograp ic as ing primitiv . or instanc , m r l g n rating t r spons as $R =$ H - (as , C) o ld b no g to pr v nt t is attack.

Thi ha bee i de e de b e ed b R e b g

ot also t at t - H r spons g n ration algorit m is also a ak link, v n n pass ords contain ad q at ntrop . It is cl ar t at t as can b r cov r d it j st t o a stiv k s arc s (abo t 2 trial d cr ptions on av rag), or in j st 9 da s sing a singl rack r mac in [il9]. nc t as is r cov r d, all ncr pt d s ssions can b r ad and t a t ntication sc m can b crack d it no ffort. is s o s t at, v n n sing 2 -bit 4 k s, t - H protocol provid s at most t q ival nt of 57-bit s c rit . is akn ss co ld also av b n avoid d b t simpl c ang s gg st d abov , $R =$ H - (as , C).

It is not cl ar to s t - H v2 d sign rs c os s c a complicat d and ins c r algorit m for g n rating 24-b t r spons s, n a simpl r and mor s c r alt rnativ as availabl .

5 - : ri i - ica r sp s

In - H v2, t rv r s nds t li nt a 2 -b t t nticator spons . li nt calc lat s t sam val , and t n compar s it it t val r c iv d from t rv r in ord r to compl t t m t al a t ntication proc ss. is val is cr at d as follo s:

. rv r (or t li nt) as s t 6-b t pass ord as it [iv9] to g t pass ord- as - as . (rv r stor s t cli nt's pass ord as d it 4; t is is t pass ord as val .)
2. rv r t n concat nat s t pass ord- as - as , t 24-b t r spons , and t lit ral string " agic s rv r to cli nt constant", and t n as s t r s lt it H .
3. rv r concat nat s t 2 -b t H o tp t from st p (2), t initial - b t g n rat d c all ng (s ction 3) and t lit ral string " ad to mak it do mor t an on it ration", and t n as s t r s lt it H .

r s lting 2 b t s ar t m t al a t nticator r spons .

5. sis

gain, t is proc ss is m c mor complicat d t an r q ir d. r is no r ason to s H t ic ; a singl as ing as t sam s c rit prop rti s.

6 al sis -

do not kno icrosoft c os s c a complicat d protocol, sinc t is is not strong r t an t follo ing:

. rv r s nds t li nt an -b t c all ng .

Thi ha bee i de e de b e ed b P e

2. li nt ncr pts t 6-b t local pass ord as it an -b t c all ng and s nds t rv r t 24-b t r spons , an -b t c all ng of its o n, and t s rnam .
3. rv r s nds a pass/fail pack t it a 24-b t r spons to t li nt's c all ng , ic is t s r's pass ord- as - as ncr pt d it t li nt's -b t c all ng .

do nsid to t - H v2 protocol is t at an av sdropp r can obtain t o copi s of t sam plaint t, ncr pt d it t o diff r nt k s. Ho v r, in t c rr nt mod l, atc ing t n t ork for an l ngt of tim ill still giv o m ltipl copi s of a s r c all ng /r spons as t s r logs in and o t, ic ill b ncr pt d it diff r nt k s.

s it stands, a passiv list n r is still abl to g t t -b t c all ng and t 24-b t r spons from t information s nt. pop lar ack r tool p tcrack [97], ic br aks indo s pass ords, orks it t is data as inp t. is task as m c asi r it - H v , sinc t ak r anag r as as s nt alongsid t strong r indo s as ; p tcrack first brok t form r and t n s d t at information to br ak t latt r [99]. p tcrack can still br ak most common pass ords from t indo s as alon [97]. nd t is still do s not solv t probl m of sing t s r's as for k ing, a t ntication, tc. it o t n gotiating, at l ast, mac in p blic k /privat k m t ods of c anging s c an important k .

6. ersi ck cks

inc icrosoft as att mpt d to r tain som back ards compatibilit it - H v , it is possibl for an attack r to mo nt a "v rsion rollback attack" against - H . In t is attack, t attack r convinc s bot t li nt and t rv r not to n gotiat t mor s c r - H v2 protocol, b t to s t l ss s c r - H v protocol.

In its doc m ntation, icrosoft claims t at t op rating s st ms ill tr to n gotiat - H v2 first, and onl drop back to - H v if t first n gotiation fails [ic99]. dditionall , it is possibl to s t t rv r to r q ir - H v2. find t is sc nario impla sibl for t o r asons. n , t soft- ar s itc s to t rn off back ards compatibilit ar r gistr s ttings, and can b diffic lt to find. nd t o, sinc old r v rsions of indo s cannot s pport - H v2, back ards compatibilit m st b t rn d on if t r ar an l gac s rs on t n t ork. concl d t at v rsion rollback attacks ar a significant t r at.

7 a s

original ncr ption m c anism in icrosoft's oint to oint ncr ption protocol ( ) s d t sam ncr ption k s in ac dir ction (li nt to rv r, and rv r to li nt). inc t b lk data ncr ption ro tin is t 4

str am cip r [c 96], t is cr at d a cr ptograp ic attack b ing t t o str ams against ac ot r and p rforming standard cr ptanal sis against t r s lt.

In t mor r c nt v rsion, t k s ar d riv d from - H v2 cr d ntials and a niq k is s d in ac dir ction. k s for ac dir c-tion ar still d riv d from t sam val (t li nt's pass ord as), b t diff r ntl d p nding on t dir ction.

7. eri i e s r - re e i s

k s can b it r 4 bits or 2 bits, and t can b d riv d from it r - H v cr d ntials or - H v2 cr d ntials. original d rivation protocol (from - H v) as d scrib d in [9]. ri fl , t pass ord as is as d again sing H , and t n tr ncat d. or a 4 -bit k , t H as is tr ncat d to 64 bits, and t n t ig -ord r 24 bits ar s t to `0xD1269E`. or a 2 -bit k , t H as is tr ncat d to 2 bits. is k is s d to ncr pt traffic from t li nt to t rv r and traffic from t rv r to t li nt, op ning a major s c rit v ln rabilit . is as b n corr ct d in - H v2.

riving k s from - H v2 cr d ntials orks as follo s:

. Has t 6-b t pass ord as , t 24-b t r spons from t - H v2 c ang , and a 27-b t constant (t string " is is t ast r K ") it H . r ncat to g t a 6-b t mast r-mast r k .
2. sing a d t rministic proc ss, conv rt t mast r-mast r k to a pair of s ssion k s.

or 4 -bit s ssion k s, t is is don as follo s:

. Has t mast r-mast r k , 4 b t s of `0x00`, an 4-b t constant and 4 b t s of `0xF2` it H . r ncat to g t an -b t o tp t.
2. t t ig -ord r 24 bits of `0xD1269E`, r s lting in a 4 -bit k .

magic constants ar diff r nt, d p nding on t r t k is s d to ncr pt traffic from t li nt to t rv r, or from t rv r to t li nt.

or 2 -bit s ssion k s, t proc ss is as follo s:

. Has t mast r-mast r k , 4 b t s of `0x00`, an 4-b t constant (magic constant 2 or 3), and 4 b t s of `0xF2` it H . r ncat to g t a 6-b t o tp t.

7. sis

is modification m ans t at niq k s ar s d in ac dir ction, b t do s not solv t s rio s probl m of ak k s. k s ar still a f nction of t pass ord, and nc contain no mor ntrop t an t pass ord. v n t o g t 4 algorit m ma t or ticall av 2 -bits of ntrop , t act al pass ords s d for k g n ration av m c l ss. is aving b n said, sing diff r nt k s in ac dir ction is still a major improv m nt in t protocol.

7. r p rs i e ic s s?

ar v r conc rn d it t magic constants mb dd d in t k d rivation algorit m for port- ak n d k s.

protocol ak ns 4 k s to 4 bits b fi ing t ig bits of t 64-bit 4 k to 0xD1269E. t t is s ms dang ro s. It is kno n t at, if an adv rsar is allo d to c oos t ig bits of t 4 k , t adv rsar can forc o into a ak k class for 4 [oo95, ag95]. r for , if t - H d sign rs—or t port-r vi r folks— ant d to mb d a trapdoor in t protocol, t co ld ploit t pr s nc of magic constants to ak n 4.

do not kno t r k s pr fi d it 0xD1269E ar n s all ak, b t in o r pr liminar statistical t sts av fo nd som s spicio s prop rti s of s c k s t at l av s s it som ca s for conc rn. o giv t o ampl s:

- mpirical m as r m nts s o t at t first f b t s of o tp t ar bias d, for k s ic start it 0xD1269E. first and s cond k str am b t s tak on t val s 0x09 and 0x00 it probabiliti s . 54 and . 6 , r sp ctiv l . is is notic abl ig r t an t /256 = . 39 probabilit o 'd p ct from good cip r.
- k sc d l mi s som ntri s in t stat tabl poorl , for t is class of k s. or instanc , $S[\ ]$ = 0xF8 olds it probabilit .3 $\approx$ $/e$, and $S[2]$ = 0x98 olds it a similar probabilit .

s statistical prop rti s ar orrisom .

ca s no information is giv n on o t val 0xD1269E as c os n, on as to orr t at it co ld ll b a "trapdoor c oic " ic forc s all 4 -bit k s into som ak k class for 4. invit t - H d sign rs to op nl disclos o all magic constants r c os n and to provid concr t ass ranc s t at t os magic val s don't cr at an idd n trapdoors. In t m antim , l av it as an op n q stion to asc rtain t r 4 is s c r n s d it t fi d k -pr fi 0xD1269E.

ack p r - ak d ri a i

In t is s ction pr s nt a v r s rio s attack on t a t at portabl 4 -bit s ssion k s ar g n rat d. is akn ss is also pr s nt in - H v as ll as - H v2, b t it as not b n discov r d ntil no .

nd r s lt is t at t so-call d "4 -bit k s" r all onl av an ff ctiv str ngt of abo t 26 bits. s a r s lt, t port- ak n d protocol can b crack d in n ar-r altim it onl a singl comp t r .

T da c e ee be ab e e ec d, hich gge ha each e ca be c ac ed i e hi g i e a a e f a h ie f a i e e a i , he e e i a e i ece a i be e gh i h a a c e f c e , he c ac i g e f a ce ca be g ea i c ea ed

r call t at t k d rivation proc ss app nds 4 s cr t bits (g n rat d in som a ic is irr l vant to o r attack) to t fi d val `0xD1269E`. r s lting 64-bit s ssion k is to 4- ncr pt t transmitt d data. probl m is t at t is proc ss introd c s no p r-s ssion salt (compar to, .g.,), and t s can b brok n it a tim -spac trad off attack.

or t r maind r of t is s ction, ass m t at can obtain a s ort s gm nt of kno n plaint t (4 bits s o ld s ffic) at som pr dictabl location. kno n plaint t n d not v n occ r at cons c tiv bit locations; t onl r q ir m nt is t at t bit positions b pr dictabl in advanc . is s ms to b a v r pla sibl ass mption, n on consid rs t q antit of kno n ad rs and ot r pr dictabl data t at is ncr pt d. t s ass m for simplicit of d scription t at t is kno n plaint t occ rs at t start of t k str am.

ill attack t is protocol it a tim -spac trad off. cost of a l ngt pr comp tation is amorti d ov r man s ssions so t at t incr m ntal cost of br aking ac additional s ssion k is r d c d to a v r lo val .

naiv attack r mig t consid r b ilding a look p tabl it 2 ntri s, listing for ac possibl 4 -bit k t val of t first 4 bits of k str am t at r s lts. is r q ir s a 2 pr comp tation, b t t n ac s bs q nt s ssion k can b brok n tr m l q ickl (it j st a singl tabl look p). Ho v r, in practic t is attack is probabl not v r practical b ca s it r q ir s 2 spac .

tim -spac trad off allo s s to r d c t spac r q ir m nts of t naiv attack b trading off m mor for additional comp tation. onsid r H llman's tim -spac trad off [H l]. or a n-bit k , H llman's trad off r q ir s a 2^n pr comp tation and $2^{n/}$ spac , and t n v r s bs q nt s ssion k can b brok n it j st $2^{n/}$ ork. (t r trad offs ar also possibl .)

or - H 's 4 -bit k s, $n = 4$, and $2n/3 \approx 26$, so o g t an attack t at br aks ac s ssion k it appro imat l 2 ork. attack r q ir s a 2 pr comp tation and 2 spac , b t t s r q ir m nts ar asil m t.

is m ans t at t port- ak n d v rsions of - H off r an ff ctiv k l ngt of onl abo t 26 bits or so, ic is m c l ss t an t claim d 4 bits of str ngt . is is a d adl akn ss.

cl si s

icrosoft as improv d to corr ct t major s c rit akn ss s d scrib d in [9]. Ho v r, t f ndam ntal akn ss of t a t ntication and ncr ption protocol is t at it is onl as s c r as t pass ord c os n b t s r. s comp t rs g t fast r and distrib t d attacks against pass ord fi l s b com mor f asibl , t list of bad pass ords—dictionar ords, ords it random capitali ation, ords it t addition of n mb rs, ords it n mb rs r placing l tt rs, r v rs d ords, acron ms, ords it t addition of p nct ation—b com s larg r. inc a t ntication and k - c ang protocols ic do not allo passiv dictionar attacks against t s r's pass ord ar possibl — ncr pt d K c ang [92, 94] and its variants

[ab96, ab97, 9], I c—it s ms impr d nt for icrosoft to contin to r l on t s c rit of pass ords. r op is t at contin s to s a d clin in s as I c b com s mor pr val nt.

r c s

S e i a d e i , c ed e cha ge: Pa d- a ed P c Sec e gai ic i a ac , *r di gs f th m- si m s r h i rit d ri* , a , 84

4 S e i a d e i , g e ed c ed e cha ge: Pa d- a ed P c Sec e gai ic i a ac a d Pa d i e i e, T&T e ab a ie , 4

i 8 i e, d , *r i g* The ec ic ie da i , Sa a ci c , , Rei a d cia e , 8

P a eh, S Pa , e hei , Taa d, a d i e, P i - -P i T e i g P c , e e af , T , h : ie f g i e e -d af d af -ie f- e - -

e 8 e a , c a a ic i e- e ade- ff, *r s ti s f rm ti h r* , T- , 4, 8 , 4 4

ab ab , S g Pa d- he ica ed e cha ge, *m t r mm i ti s i* , c , 5

ab ab , e ded Pa d e cha ge P c e ic i - a ac , *r di gs f th i th r sh i g h gi s fr str t r f r r ti t r ris s*, e S cie , , 48 55

h ea d ie , c , h ac Tech ica Ra , h : h c h c ac a h

h ea d ie , c, h c ac , , h : h c h c ac

ic a ic f a i , d a ced i d T ce , e Ri- de P b i hi g, Re e a cha e a h : ic f c c ica i h

ic b ic f a i , P i - -P i T e i g P c PPTP e- e ed Q e i ,

ic 8a ic f a i , e e ed Q e i ab ic f P Sec i , ec 8, h : ic f c TSe e c e de e ei f P Sec_ Q a

ic 8b ic f a i , ic f i d 5 ia -U e i g U g ade Re ea e e , 8, h : ic f c b a ic e 54 a

ic ic f , a i , i d 8 ia -U e i g Sec i U g ade Re ea e e , eb , h : ic f c b a ic e Q 8 a

ST a i a i e f S a da d a d Tech g , Sec e a h S a da d, US e a e f e ce, a

PZ 8 S Pa a d Z , ic f P i - -P i c i PP P c , e i g , e e af , T , a 8 h : ie f g i e e -d af d af -ie f- e - e-

Ri R Ri e , The 4 e age ige g i h , d a ce i g — RYPT P ceedi g , S i ge - e ag, ,

R 5 R , ea e i R 4, ci c , Se 5

Si 4 Si , The P i - -P i P c PPP , e i g , ST 5 , R , 4 f : f i i ed i - e fc

Sch Sch eie , ied g a h , d di i , h i e & S ,

S 8 Sch eie a d dge, a a i f ic f P i - -P i T e i g P c PPTP , *r di gs f th th f r mm i ti s d m t r rit* , P e , 4 h : c e a e c h

ag 5 ag e , Re: ea e i R 4, ci c , 5 Se 5 h : c be e e ed da - - c4- ea - e

8 T , The Sec e Re e Pa d P c , *r di gs f th t r t i t t r d istri t d st m rit m si m*, a 8,

Z 8 Z a d S bb, ic f PPP P e i , e i g e e af , a 8 h : ie f g i e e -d af d af - ie f- e - cha -

Z 8a Z , e i i g PP e f S- P ede ia , e - i g e e af , Se 8 h : ie f g i e e - d af d af -ie f- e - cha - e -

Z 8b Z , e i i g PP e f S- P ede ia , e - i g e e af , 8 h : ie f g i e e - d af d af -ie f- e - cha - e -

Z Z , ic f PPP P e i , e i , e i g e e af , h : ie f g i e e -d af d af - ie f- e - cha - -

t -r c ra l t -c rti a l r pt s st s (r)

dam Yo ng and oti Y ng

e b a U e
e e

h a e e e he ece -Rec e ab e
- e fiab e e Th ha bee f h e
he f a e e e c b e a effic e a e h he
c e f a P b c e f a c e P Th e e e he
e ac ec fica f he b e h ch ba e ha f a e e
e c ca h e ach e e The ec fica a e e a a e he
ffic ech ca e he a ea f he e ha a e ee-
g ffic e he e e he E c 8 a P ,
h ch g e a effic e e c a f a e e e c e f
a ce fie b c e e P a e , e h h c c
a e c e P f e e a he a e c a eff e e f a
eg a P e ec fica , he che e e e e a e a effic e f
e e a a P , e e a e - e a ha a e e ,
he ca be b e f a e e , a he che e a e ha-
b c e e a a efi e 5 b a a e gh
a e , he a he e b h b c e he he
he e ce fie The che e e ab e he effic e e fica f he
fac ha a g e e a e e e c e e The a he
afe a effic e ec e f e a a e e age h ch -
ca e e ge c a ch a he e ca a ea, ec e fi e
e , a c a e ga e c e ha e a -
ca e ea h he c e ega g he ee f g e e
c acce e age a h gh ech ca ca e
ha e c e e ee e e e e effec
he e a P e e e he b efl e f hc g
e e e he a ea h ch c e f he fle b c a b
e e e f a - ec e ab e c e , a e a e g f
ch e h ch a e ba e a a b c e e h RS
a c e e g

I tr cti

ar c rr ntl at th point, d to th normo s s rg of Int rn t s , h r a larg -scal blic K Infrastr ct r (KI) is abo t to b d plo d. n th oth r hand, anoth r s t of r q ir m nts s gg st that d cr ption k s sho ld b

. au gar (d.): ’ , 7 , pp. – , .

scro d. his is asil j sti abl in orld id d plo m nt of s st ms h r m dical r cords can b acc ss d, t picall b th cli nt, b t onl in an m rg nc sing scro m chanisms. lso, go rnm nts ar int r st d in s c ring acc ss to t l phon s st ms for la nforc m nt (this last iss is politicall contro r-sial, b t o r tr atm nt is onl t chnical). ost if not all of th arl propos d k scro sch m s s ff r from at l ast on form of dra back or anoth r (t pi-call from inh r nt incompatibiliti s ith soft ar bas d r g lar KIs). h s incl d th n d for "tamp r-r sistant" d ic s, .g., lipp r and apston , ad-d d o rh ad of protocol int raction b t n s rs and th scro a thoriti s, th n d for "tr st d third parti s" to g n rat cr ptographic k s and b ac-ti in th s r-to- s r transactions, and r q iring chang s in protocols hich ar o tsid th cr ptographic s st m.

In fact, th probl m of impl m nting an scro d KI ffici ntl is r gard d as too diffic lt a probl m to achi b a n mb r of r s arch rs, cr ptograph rs, and s c rit p rts [K-]. In anoth r pap r [Y97], formal arg m nts ar pr - s nt d plaining h b ilding k scro on top of a p blic-k s st m is a non-tri ial task (n h n third parti s ar allo d to b pr s nt). h arl at-t mpts to pr s nt scro d ncr ption, ind d, propos d s st ms m ch diff r nt than a r g lar KI. to- co rabl to- rti abl cr ptos st ms att mpt to sol th ffici nc (and compatibilit) probl ms that ar pos d to scro d KI's, and do not claim to r sol th ongoing conflict b t n pri ac ad ocat s and thos s king acc ss to scro d k s. r mark that nlik r c nt scro proposals hich gi th scro a thoriti s onl acc ss to som fraction of th scro d information (.g., as in [97]), to- co rabl to- rti abl cr ptos st ms gi th scro a thoriti s acc ss to all ncr pt d information h n a thori d. Ho r, th acc ss do s not ha to b to a k , rath r it can ha r small gran larit hich nabl s acc ss to an indi id al m ssag . b li that gran lar acc ss [Y95] is mor acc ptabl than partial acc ss hich impli s f rth r comp tational costs in r co ring th m ssag (th cost ff cti n ss is not j sti d from an ngin ring point of i and th d la of partial r co r ma not b tol rabl).

I itial r l p ci cati

h follo ing ar sp ci cations of soft ar scro d KI as can b d ri d from isting doc m nts, disc ssions in th cr ptographic comm nit , and approach s to s st ms d lopm nt:

. **t ar i pl tati** ach and r s st m compon nt do s not r q ir tamp r-proof hard ar .
2. **t ar distrib ti** h soft ar that s rs mplo is p blic (and h nc is asil distrib t d).
3. **K s l -g rati** s rs g n rat th ir o n pri at k s ind p nd ntl and ffici ntl . h pri at k s (or m ssag s ncr pt d b th s k s) ar r co rabl b th scro a thoriti s onl .

4. **s r a t riti s i i al i t r ti** h scro a thoriti s act onl at th s st m's s t- p, and h n k r co r is n d d.
5. **KI- patibl rti ati pr ss** o c rtif a k , a s r s nds on m ssag r q sting c rti cation to th rti cation thorit ( ), as in a r g lar p blic k infrastr ct r . his m ssag is cr at d b an ffici nt proc d r , p rform d ind p nd ntl b th s r alon .
6. **rti d k s ar r rabl** s r's p blic k is c rti d b a r- ti cation thorit ( ) onl if th corr sponding pri at k is ri d to b r co rabl b th a thoriti s. his ri cation is cond ct d sol l from th m ssag that forms th r q st for c rti cation; th ri cation is s cc ssf ll if and onl if th k is r co rabl ith r high probabilit .
7. **KI- patibl rti at s** s r's k in th c rti cat sho ld incl d th sam information as in a r g lar p blic k .
. **i rsal ri abilit r rabilit** pon r q st, a s r can pr - s nt th m ssag that forms th r q st for c rti cation to an part and this part can rif that th pri at k is r co rabl b th a thoriti s.
9. **ffi i t r r** h k r co r proc d r is ffici nt (it can pr f ra- bl b don b distrib t d parti s, .g., sing thr shold cr ptograph [9] and ri abl s cr t sharing hich ha b n d lop d in th 's).
. **KI- patibl s r s st** h s st m is as as for s rs as a p - blic k cr ptos st m, and can b impl m nt d in soft ar . ch a sol tion th r for constit t s a r d ction of a KI ith a rti cation thorit [Koh7] to an scro d p blic k infrastr ct r ith th sam con g ra- tion. inc s ch a sol tion can b impl m nt d s c r l in soft ar , it can b impl m nt d and distrib t d in so rc cod form, th s making it as as to distrib t and s as a p blic k soft ar packag (.g.,).
. **KI- patibl s t ar /ar it t r la rs** rom an infrastr ct r and s st ms int gration p rsp cti , th s sp ci cations diff r ntiat b t- n ario s ind p nd nt la rs. h rst la r consists of th scro a t- horiti s, ho act onl at th tim th s st m is stablish d and ho act onl h n a pri at k n ds to b r co r d. h lat r action is p rform d ith- o t int rfacing ith s rs. h s cond la r is th p blic-k infrastr ct r , h r s rs and 's g n rat c rti d k s hos corr sponding pri at k s ar pri at to th s rs. h third la r is th s of th c rti d p blic k s ithin comm nication and storag applications. In s ch a s st m th third la r is r lat d to th s cond la r as in a r g lar p blic k infrastr c- t r .
2. **i ati r t l patibilit** h sol tion sho ld not chang h ad rs and m ssag s o tsid th KI protocols; .g., comm nicating parti s s isting comm nication protocols.
3. **plia ass ra** In [Y95, Y97] rank l and Y ng not that an scro ncr ption sch m can al a s b b pass d (hard ar or soft ar). his is d to nd r- ncr pting, o r- ncr pting, tc. h s, go rnm nts cannot hop to sol misb ha iors in g n ral. hat is important is th d nition gi n in [Y95] hich sa s that "as long as th parti s mplo th m chanisms pro id d for con d ntialit b th s st m, th scro capabilit

sho ld b nabl d". In an to- co rabl to- rti abl s st m, th ti s th c rti cation of k s to ass r that s cr t k s ar scro d. It s ms that this is a prop r choic of control sinc in ord r to b pass th s st m, s rs ill ha to s anoth r s st m or s an na thori d modi cation of th s st m. lso, not p rforming th 'ass ranc of scro ' b th at th infrastr ct r l l ma ca s probl ms in s st m d sign, as point d o t in [Y97].

4. **rit** h p blic k is as s c r as a k in a KI against all parti s ([YY9] and [YY99]r q ir an additional ass mption for ach, b t onl for arg ing s c rit against th , h r as it is possibl to r d c th s c rit of th k to a kno n ass mption, oth r is).

5. **ad -p bli -k r sista** noth r asp ct of s c rit is that th s st m sho ld not contain a s bliminal chann l that nabl s "shado p blic-k " distrib tion [K 95]. ch a prop rt is hard to pro , b t at th r l ast it sho ld b r q ir d that hat is p blish d to th g n ral p blic in th k scro s st m is th sam information as hat is p blish d in a r g lar p blic k s st m.

h r ar thr additional r q ir m nts hich ar oft n d sir d in man applications:

6. **st** n d to ha th s st m b of r lati lo r so rc cost. In partic lar, h r as th s r sho ld ha no additional cost h n compar d to an n scro d KI s r, th ma ha som additional cost (.g., a mod rat incr as in m mor and proc ssing, tho gh this m mor ma b maintain d at th scro a thoriti s as ll) and th onl r al additional cost is in managing and op rating th scro a thoriti s (hich is a r q i-r d cost). t pical cost of th a thoriti s and th n ds for th ir s c rit sho ld b compatibl ith th corr sponding cost and n ds of a (p rhaps distrib t d) .

7. **ra larit s r** noth r prop rt hich ma b r q ir d is that rath r than op ning k s of s rs, th a thoriti s op n s ssion k s hich ar ncr pt d nd r th p blic k s of s rs. h s ssion k is op nabl r gardl ss of hich of th t o s rs in th s ssion has b n a thori d as a targ t for k scro . h notion of gran larit in taking a k o t of scro as d alt ith in [Y94, Y95] and b nstra, inkl r, and Yacobi [Y95]. his prop rt is t picall a f nction of th k of th scro a thorit (b t can b al a s achi d if th a thoriti s, rath r than a larg n mb r of s rs, ar impl m nt d in tamp r-proof hard ar).

. **as t s r tr st** In a KI s tting th s st m's tr st is ith th ; it ma b d sirabl in an scro KI s tting that tr st r main ith th . In to- co rabl to- rti abl cr ptos st ms it is possibl for th to r tain critical scro d information for ach s r (tho gh th cannot acc ss it), and th s collaboration can b mad n c ssar to tak information o t of scro , th s making th tr st r main ith th .

t - c ra l t - rti a l r pt s st s: ral tr ct r

h pap rs [YY9] and [YY99] d scrib t o diff r nt to- co rabl to- rti abl r ptos st ms s ch that h n ach is r n an l amal [l 5] p - blic/pri at k pair, an scro d ncr ption of th pri at k , and a proof that th scro a thoriti s can r co r th pri at k is prod c d for th s r. h proof, in addition to th ' ncr ption' of th pri at k , has b n call d a **rti at r rabilit** . his c rti cat is p blicl ri abl and ass - r s that th pri at k is scro d prop rl . In short, ach algorithm d scrib s ho to constr ct a string hich constit t s an implicit ncr ption of th pri at k x nd r th scro a thoriti s k and a non-int racti ro-kno l dg (IZK) proof that allo s a pro r to pro to a ri r that h r pri at k x in $y = g^x$ mod p is th sam as in th implicit ncr ption. H nc , a rti ca- tion thorit ( ) can insist that a s r ho s bmits h r o n p blic k for p blication also s bmits th c rti cat j st d scrib d. Ha ing don so, th can b c rtain that x is scro d prop rl , itho t r l arning x its lf. h primar diff r nc b t n th t o algorithms is that th p blic k of th s- cro a thoriti s in [YY9] is a discr t log bas d p blic k , h r as in [YY99] it is an mod l s.

mphasi that th proofs and ncr ptions mplo d ar ffici nt and do not contain ncr ptions of circ its and g n ral proofs hich mplo s ch con- str ctions (hich ar t picall pla sibilit r s lts rath r than act al s st ms). nc th k s ar c rti d b th , th ir s ithin th s st m is as in a r g lar KI bas d on l amal/ iffi -H llman k s. K r co r is an ffici nt proc d r b t n th and th scro a thoriti s, ho ar oth r is not acti . h coop ration ith th is n d d, t th cannot r co r th k s.

or s c rit th primar cr ptographic ass mption that is mad is that th iffi -H llman (H) probl m is hard. his ass mption is s d for s c rit against ad rsari s. or th s r to b s c r from th , ach of th afo- r m ntion d to- co rabl to- rti abl r ptos st ms r q ir s a n cr ptographic ass mption. ot that th H ass mption is alr ad r q ir d b - ca s th l amal K is s c r if and onl if th H probl m is hard. to th non-int racti nat r of th c rti cat s of r co rabilit , a random oracl cr ptographic hash ass mption (for H) is also r q ir d for th alidit of th proofs ithin th c rti cat .

h c rti cat of r co rabilit to th is not mad p blic to a oid shado p blic ab s .

lat d rk

ario s tamp r-r sistant hard ar sol tions ha b n propos d, lik th . . go rnm nt's lipp r chip and apston chip. h s sol tions ar nd sirabl for s rs sinc th r q ir sp cial hard ar , and sinc s cr t nscr tini d

algorithms ha to b tr st d. ([YY96,YY97a,YY97b] for pot ntial probl ms ith s ch d signs). lso, attacks has b n fo nd (.g., [Y95]).

air blic K r ptos st ms (K) is a p blic k scro s st m that can b impl m nt d in soft ar [i92]. n of th probl ms ith K 's is that r s r m st split his or h r pri at k and s nd th shar s to th a thoriti s. h a thoriti s m st th n int ract to ins r that th k is scro d. o, th s st m has mor comm nication o rh ad than a t pical p blic k s st m. lso, K 's can b ab s d ia th s of shado p blic k cr ptos st ms, as sho n b Kilian and ighton [K 95]. Kilian and ighton propos d a k scro sol tion call d ailsaf K scro (K) to th shado p blic k ab s probl m. Ho r, in so doing K 's r q ir n mor protocol int raction to scro k s than K 's.

" ra d- t ctabl lt rnati to K - scro roposals" bas d on l a-mal as d scrib d in [97]. his s st m, call d binding l amal, allo s s rs to s nd ncr pt d information along ith a pol -si d proof that th s ssion k that as s d in th ncr ption can b r co r d b th scro a thoriti s. It as point d o t in t o diff r nt r mp s ssion pr s ntations at rocr pt '97 that it is possibl to s th m ans pro id d b th binding l amal s st m to d f at th scro capabilit [97, 97].

iti s

Informall , an to- co rabl and to- rti abl cr ptos st m is a s st m that allo s a s r to g n rat a to-c rti abl k s (k s ith a proof of th m thod of g n ration) ffici ntl . h follo ing is a formal d nition.

iti . *t - c ra l a t - rtifia l r t s st m is a tri-l (REC) (h r REC ma a m-t l (REC REC ... REC_m) s ch that*

. is a licl l -tim r a ilistic ri g achi that ta s i t a g rat s th tri l (K K P) hich is l ft th ta as t t. H r K is a ra ml g rat ri at a K is th c rr s i g lic . P is a l -si c rtificat that r s that K is r c ra l th scr a th riti s si g P.

2. is a licl l -tim t rmi istic ri g achi that ta-s (K P) its i t ta a r t r s a l a al . ith r high r a ilit r t r s tr iff P ca s t r c r th ri at K .

3. REC is a t rmi istic ri g machi ith a ri at i t. r a istri-t im l m tati REC_i h r i m is a l -tim t rmi istic ri g achi ith a ri at i t that ta s P as i t a r t r s shar i f K its ta as t t ass mi g that K as r rl scr . (-s ts f) th ri g achi s REC_i f r i m ca s c lla rati l t r c r K .

. It is i tracta l t r c r K gi K a P ith t REC (r REC ... REC_m).

t ill d n informall th st ps tak n in a blic K Infrastr ct r (KI) and in an to- co rabl to- rti abl KI. h follo ing is th str ct r (protocol) of a blic K Infrastr ct r :

. 's addr ss s and param t rs ar p blish d and distrib t d.
   a) ach s r g n rat s a p blic/pri at k pair, and s bmits th p blic k , along ith an I string, to a .
   b) h ri s th I string, c rti s th p blic k (b signing it), and nt rs th c rti cation in th p blic k databas .
   c) o s nd a m ssag , a s r q ri s th to obtain th p blic k of th r cipi nt, and ri s th signat r of th on th p blic k .
   d) h s r th n ncr pts th m ssag ith th r cipi nts p blic k and s nds th corr sponding ciph rt t to th r cipi nt.
) h r cipi nt d cr pts th ciph rt t ith his or h r o n pri at k .

h follo ing is an to- co rabl to- rti abl KI:

. s t of s st m param t rs ar agr d pon. h scro a thoriti s g n rat an scro ing p blic k ith corr sponding pri at shar s. h p blic param t rs and 's param t rs ar distrib t d (.g., in soft ar).
   a) ach s r g n rat s a p blic/pri at k pair, and s bmits th p blic k along ith an I string and a c rti cat of r co rabilit , to a .
   b) sing th scro ing p blic k , th ri s th c rti cat of r co-rabilit . ro id d that this ri cation holds, and that th I string is alid, th c rti s th p blic k (b signing it), and nt rs th c rti cation in th p blic k databas .
   c) o s nd a m ssag , a s r q ri s th to obtain th p blic k of th r cipi nt, and ri s th signat r of th on th p blic k .
   d) h s r th n ncr pts th m ssag ith th r cipi nts p blic k and s nds th corr sponding ciph rt t to th r cipi nt.
) h r cipi nt d cr pts th ciph rt t ith his or h r o n pri at k .
2. If a ir -tap is a thori d for a gi n s r, th scro a thoriti s obtain th c rti cat of r co rabilit of that s r (from th), and r co r th k or cl art t nd r th k .

ot that (a) thro gh ( ) abo ar f nctionall q i al nt in both s st ms. h onl diff r nc is that in th scro s st m, th is abl to rif that th pri at k is r co rabl b th scro a thoriti s. h onl add d it ms in th a to r co rabl KI to hat is r q ir d for a KI ar s t- p tra ork in st p and st p 2. st p 2 is n c ssar b d nition and st p additional ork s ms n c ssar to bind th s st m to th scro a thoriti s.

In an to- co rabl to- rti abl s st m, th i-th scro a thorit EA_i kno s onl REC_i, in addition to hat is p blicl kno n. o p blish a p blic k , s r r ns () and r c i s (K ,K ,P). k ps K pri at and s nds th pair (K ,P) to th . h th n comp t s (K ,P), and p blish s a sign d rsion of K in th databas of p blic k s iff th r s lt is tr . th r is , 's s bmission is ignor d. In ith r cas th c rti cat of r co rabilit is not p blish d. ppos that 's p blic k is acc pt d and K

app ars in th databas of th . i n P obtain d from th , th scro a thoriti s can r co r K as follo s. EA_i comp t s shar i of K b r nning $REC_i(P)$. h a thoriti s th n pool th ir shar s and r co r K .

t - c ra l t - rti a l r pt s st s

5. s r ( )

at ati al r li i ari s t Z_q d not th m ltiplicati gro p of canonical l m nts r lati l prim to $2q$ (s d it to call th gro p and its l m nts). H r q is a larg odd prim . It is straightfor ard to sho that Z_q is a c clic gro p (it poss ss s a primiti root). In fact, if s is a primiti root mod lo q and if s is odd, th n s is also a primiti root mod lo $2q$. If s is a primiti root mod lo q and s is n, th n $s+q$ is a primiti root mod lo $2q$. [o93] for d tails. It can b sho n that th r ists a g n rator s for all gro ps Z_q. h s, th r is a probabilistic pol -tim algorithm to nd a g n rator of Z_q. h follo ing rst t o simpl claims ar s d to sho that if discr t log probl m is hard, th n th discr t log probl m in Z_q is hard.

laim. $(s^k \ mod\ 2q)\ mod\ q = s^k\ mod\ q$.

laim. If $(s^k \ mod\ 2q) = s^k\ mod\ q$, th n $k = k$.

laim. If H mod q is hard, th n H mod $2q$ is hard.

r f. ill pro this b pro ing th contrapositi . ppos ar gi n a bo that tak s A and B and r t rns $s^{ab}\ mod\ 2q$ h r $A = s^a\ mod\ 2q$ and $B = s^b\ mod\ 2q$. n d to sho that can s to p rform H gi n $A = s^a\ mod\ q$ and $B = s^b\ mod\ q$. o do this, choos r , r $_R\ Z_{q-}$ s ch that A^r and B^r ar odd mod q, pro id d that s is odd (if s is n, mak s r th s t o al s ar n). th n comp t $t = X(A^r\ mod\ q, B^r\ mod\ q)$. laim 2 it follo s that $t = s^{a\ b\ r\ r}\ mod\ q$. th n o tp t $t^{(r\ r\ )^-}\ mod\ q$. ot that $r\ r$ has a niq in rs mod $q-$ sinc r , r Z_{q-} . r algorithm th s o tp ts $s^{a\ b}\ mod\ q$ as n d d. .

rom laim 3 it follo s that if th H probl m is hard, th n th discr t log probl m in Z_q is hard.

robl m : t $p = 2q +$ and l t $q = 2r +$ h r p, q, and r ar prim . ind $t^k\ mod\ 2q$ gi n $s^k\ mod\ 2q$ and $g^{t^k}\ mod\ p$. H r g, s, t, and p ar p blic. g g n rat s Z_p, s g n rat s Z_q, and t g n rat s a larg s bgro p of Z_q.

h diffic lt of robl m is a cr ptographic ass mption in [YY9]. l arl , robl m is not hard if th discr t -log probl m is not hard, or if H is not hard.

not that tadl r [t96] has initiat d th s of th do bl -d ck r ponntiation in his p blicl - ri abl s cr t sharing ( ) ork prior to o r s of it. H also not s that his can b s d in th mod l of icali's " air r ptos st ms". Ho r, this m ans that th application s ff rs from th similar probl ms of th original fair cr ptos st ms hich o r ork has att mpt d to o rcom .

st t p larg prim r is agr d pon s.t. $q = 2r+$ is prim and s.t. $p = 2q+$ is prim . ha prod c d s ch larg al s ffici ntl . g n rator g is agr d pon s.t. g g n rat s Z_p, and an odd al g is agr d pon s.t. g g n rat s Z_{q}. h al s $(p,q,r,g,g\ )$ ar mad p blic.

n ampl of organi ing th scro a thoriti s is gi n; oth r s ttings of thr shold sch m s or n sch m s h r s rs d cid on hich a thoriti s to b ndl tog th r ar possibl . h r ar m a thoriti s. ach a thorit EA_i choos s z_i $_R$ Z_{r}. h ach comp t $Y_i = g^{\ z_i}\ mod\ 2q$. h th n pool th ir shar s Y_i and comp t th prod ct $Y = \prod_{i=}^{m} Y_i\ mod\ 2q$. ot that $Y = g^{\ z}\ mod\ 2q$, h r $z = \sum_{i=}^{m} z_i\ mod\ 2r$. h a thoriti s choos th ir z_i o r again if $(g\ /Y)\ mod\ 2q$ is not a g n rator of Z_{q}. ach a thorit EA_i k ps z_i pri at . h p blic k of th a thoriti s is $(Y,g\ ,2q)$. h corr sponding shar d pri at k is z.

K rati s s "do bl d ck r" pon ntiation and op rat s as follo s. It choos s a al k $_R$ Z_{r} and comp t s $C = g^{\ k}\ mod\ 2q$. th n sol s for th s r's pri at k x in $Y^k x = g^{\ k}\ mod\ 2q$. comp t s th p blic k $y = g^x\ mod\ p$. comp t s a portion of th c rti cat v to b $g^{Y^{-k}}\ mod\ p$. also comp t s thr IZK proof transcript P , P , P (hich ar g n rat d b th IZK proof s st ms $ZKIP$, $ZKIP$, and $ZKIP$, d scrib d b lo). h c rti cat P is th 5-t pl $(C,v,P\ ,P\ ,P\ )$. l a s $((y,g,p),x,P)$ on th o tp t tap (not that y n d not b o tp t b th d ic sinc $y = v^C\ mod\ p$). h s r's p blic k is (y,g,p).

bli s r ri ati tak s $((y,g,p),P)$ on its inp t tap and o tp ts a bool an al . ri s th follo ing things:

. P is alid, hich sho s that kno s k in C
2. P is alid, hich sho s that kno s k in v
3. P is alid, hich sho s that kno s k in $v^C\ mod\ p$
4. ri s that $y = v^C\ mod\ p$

r t rns tr iff all 4 crit rion ar satis d. P is ss ntiall th sam as th proof d scrib d rst in [HY 5] for isomorphic f nctions, b t th op rations h r ar in Z_{q}. $ZKIP$, hich is th basis for P and P , ill b plain d in th follo ing s ction.

In $ZKIP$, th pro r ish s to int racti l pro to a ri r that th pro r kno s k in $T = g^{s^k}\ mod\ p$. It is ass m d that th ri r do s not kno $s^k\ mod\ 2q$ (and h nc h do sn't kno k). h al s T, g, s, and p ar p blic. h q antit g g n rat s Z_p. h follo ing thr -pass protocol is r p at d n tim s.

. h pro r choos s e $_R$ Z_{r} and s nds $I = T^{s^e}\ mod\ p$ to th ri r.
2. h ri r s nds b $_R$ Z to th pro r.
3. h pro r s nds $z = e + bk\ mod\ 2r$ to th ri r.
4. h ri r ri s that $I = (T^{\ -b} g^b)^{s^z}\ mod\ p$.

h ri r acc pts th proof iff st p 4 pass s in all n ro nds of th protocol. $ZKIP$ is a thr -pass protocol that s s al s (I,b,z) hich ar r similar to th al s (I,b,z) hich ar s d in $ZKIP$.

It r mains to sho ho th IZK proofs in P ar constr ct d. t $e_{i,j}$ d not th pro r's random choic for it ration j of proof P_i. H r i 3 and j n.

. $P = (C,v)$

2. h pro r choos s al s e , , e , , ..., e $_{,n}$, e , , e , , ..., e $_{,n}$,e , , e , , ...,e $_{,n}$ $_R$ Z $_r$. ot that th e's m st b in Z $_r$, oth r is information abo t k ma b l ak d in st p ( ). o s this, not that e is n d d to blind kb p rf ctl .
3. h pro r comp t s $I_{,j} = g^{e_{,j}}$ mod $2q$, $I_{,j} = v^{Y^{-e_{,j}}}$ mod p, and $I_{,j} = y^{(g/Y)^{e_{,j}}}$ mod p for j n
4. h pro r incl d s all th al s $I_{i,j}$ in P, h r i 3 and j n.
5. h pro r comp t s

$$rnd = H(I_{,}, I_{,}, ..., I_{,n}, I_{,}, I_{,}, ..., I_{,n}, I_{,}, I_{,}, ..., I_{,n})$$

h r H is a cr ptographic on - a f nction.

6. h pro r g ts th $3n$ al s $b_{i,j}$ for i 3 and j n from th $3n$ l ast signi cant bits of rnd. h s ar th chall ng bits. ot that th ri r can calc lat th s bits gi n th al s for I.
7. h pro r comp t s $z_{i,j} = e_{i,j} + b_{i,j}k$ for i 3 and j n.

. h pro r incl d s th al s $z_{i,j}$ in P, h r i 3 and j n.

h ri r acc pts th proof iff all $3n$ ch cks pass and if $y = v^C$ mod p. his m thod of making a ZKI non-int racti is d to iat and hamir [6].

K **r** REC_i r co rs shar i of th s r's pri at k x as follo s. REC_i tak s C from P. It th n comp t s shar s_i to b C^{z_i} mod $2q$, and o tp ts s_i on its tap . h a thoriti s th n pool th ir shar s and ach comp t s $Y^k = \prod_{i=}^{m} s_i$ mod $2q$. rom this th can ach comp t $x = CY^{-k}$ mod $2q$, hich is th s r's pri at k .

h scro a thoriti s can r co r th plaint t of s rs s sp ct d of criminal acti it itho t r co ring th s r's pri at k its lf. o d cr pt th ciph rt t (a, b) of s r U th scro a thoriti s proc d as follo s:

. ach of th m scro a thoriti s i r c i s C corr sponding to U.
2. scro a thorit comp t s s $= a^{C^{-z}}$ mod p.
3. scro a thorit $i+$ comp t s s_i $= s_i{}^{C^{-z_i}}$ mod p.
4. scro a thorit m d cr pts (a, b) b comp ting $b/(s_m{}^C)$ mod p.

his s st m allo s for m ltipl 's to b associat d ith th scro a thoriti s. scro ing across scro a thoriti s domains (.g., diff r nt co ntri s) can b sol d b th s rs mplo ing th long-li d iffi -H llman k as th ir

common k (hich is r co rabl b ith r co ntr) or b bilat ral agr m nts. or proofs of s c rit r f r th r ad r to [YY9].

ot that onl th s r's p blic k is p blish d as in a r g lar p blic k s st m. In fact, it is insist d that th c rti cat of r co rabilit not b p blish d. his is to pr nt th stablishm nt of a shado p blic-k for ach s r.

5. s r ( )

at ati al r li i ari s h s st m r q ir s th follo ing cr ptographic ass mption.

robl m 2: itho t kno ing th factori ation of n, nd x h r x Z_{tn}, gi n x^e *mod* $2tn$ and g^x *mod* p. H r , $p = 2tn +$, $n = qr$, p, q, r, and larg prim s,t is a small prim , g g n rat s a larg s bgro p of Z_p, and gcd(e,$\phi(tn)$) = . In this ork $e = 3$.

It is also ass m d that it is hard to comp t th ntir plaint t if r d ctions ar p rform d mod lo $2tn$, as oppos d to r d cing mod lo n as in . call that t is a small prim n mb r .

Int iti l , it s ms that probl m 2 sho ld b hard, sinc x^e *mod* $2tn$ is a pr s m d on - a trapdoor f nction of x, and g^x *mod* p is a pr s m d on - a f nction of x. l arl , robl m 2 is not hard if cracking is not hard, or if comp ting discr t logs is not hard.

st t p h scro a thorit (a thoriti s) g n rat a shar d l m int g r $n = qr$, h r q and r ar prim . h scro a thoriti s th n mak s r that gcd(3,$\phi(n)$) = . If this condition do s not hold, th n th scro a thoriti s g n rat a n n. h scro a thoriti s th n comp t $p = 2tn +$, h r t is dra n from th rst, sa 256 strong prim s starting from , incl si . If p is fo nd to b prim sing on of th s al s for t, th n th al s for n and p ha b n fo nd. If non of th al s for t ca s s p to b prim , this ntir proc ss is r p at d as man tim s as n c ssar . ot that $t = 2t +$ h r t is prim . inc insist that $t > 7$, ar g arant d that gcd(3,$\phi(tn)$) = . nc n and p ar fo nd, th scro a thoriti s g n rat th pri at shar s d ,d ,...,d_m corr sponding to $e = 3$. al g $_R$ Z_{tn} is chos n s ch that g has an ord r that is at l ast as larg as th small st of q and r, in th ld Z_p (r call that th factori ation of n is not kno n). h al s t, n, and g ar mad p blic.

his s st m can b s t p m ch fast r than [YY9] sinc th scro a thorit can g n rat a composit mod l s r q ickl , and in ord r to nd a prim p, t can b ari d as n d d. h p ct d tim to nd s ch a p is in rs l proportional to th d nsit of prim s. In contrast, in [YY9] th s st m s t p r li d on nding thr prim s ith a rigid r lationship b t n th m. H ristic l this m ans that sampling s ch prim s ma tak an p ct d tim hich is in rs l proportional to th d nsit of th prim s c b d.

---

he ca be g e he a e a he e ca a a ch e a e h ch a e fi e a

K rati op rat s as follo s. It choos s a al x $_R Z_{tn}$ and comp t s $C = x$ $mod\ 2tn$. x is th s r's l amal pri at k . th n comp t s $y = g^x\ mod\ p$. h s r's l amal p blic k is (y, g, p). ot that g ma not n c ssaril g n rat Z_p, b t, can mak s r that it g n rat s a larg s bgro p of Z_p. also comp t s a non-int racti ro-kno l dg proof bas d on C and y. h follo ing is ho this proof is constr ct d.

. choos r , r , ..., r_N $_R Z_{tn}$.
2. comp t $C_i = r_i$ $mod\ 2tn$ for i N
3. comp t $v_i = y^{r_i}\ mod\ p$ for i N
4. $b = H((C\ , v\ ), (C\ , v\ ), ..., (C_N, v_N))\ mod\ 2^N$
5. $b_i = (2^i\ AND\ b) >$ for i N
6. $z_i = r_i x^{\ b_i}\ mod\ 2tn$ for i N

H r N is th n mb r of it rations in th IZK proof (.g., $N = 4$). on-c rning st p , t chnicall th pro r has a chanc that on of th r_i ill ha q or r in its factori ation, this is highl nlik l . ot that b_i in st p 5 r s lts from a bool an t st. b_i is if h n tak th logical of 2^i and b g t a al gr at r than ro. It is oth r is . h proof P is $(C, (C\ , v\ ), (C\ , v\ ), ..., (C_N, v_N), z\ , z\ , ..., z_N)$. l a s (($y$,$g$,$p$),$x$,$P$) on th o tp t tap .

bli s r ri ati tak s ((y,g,p),P) on its inp t tap and o tp ts a bool an al . ri s th follo ing things:

. $C^{b_i} C_i = z_i$ $mod\ 2tn$ for i N
2. $v_i = (y^{\ -b_i} g^{b_i})^{z_i}\ mod\ p$ for i N

r t rns tr both crit rion ar satis d. ot that sk ptical ri rs ma also ish to ch ck th param t rs s ppli d b th scro a thoriti s (.g., that n is composit , p is prim , tc.).

K r REC_i r co rs shar i of th s r's pri at k x as follo s. REC_i tak s C from P. It th n r co rs shar s_i sing th pri at shar d_i. It o tp ts s_i on its tap . h a thoriti s th n pool th ir shar s and x is comp t d.

ri g lai t t ata h scro a thoriti s can r co r th plaint t of s rs s sp ct d of criminal acti it itho t r co ring th s r's pri at k its lf. In this s ction, it is ass m d that th m thod b ing s d is [97]. In this cas th pri at d cr ption pon nt is $d = \sum_{i=}^{m} d_i\ mod\ \phi(tn)$, and d is th in rs of 3 mod $\phi(tn)$. o d cr pt th l amal ciph rt t (a, b) of a s r U th scro a thoriti s proc d as follo s:

. ach of th m scro a thoriti s r c i s C corr sponding to U.
2. scro a thorit comp t s $s\ = a^{C^d}$ $mod\ p$.
3. scro a thorit $i +$ comp t s s_i $= s_i^{\ C^{d_i}}$ $mod\ p$.
4. scro a thorit m d cr pts (a, b) b comp ting $b/(s_{m-}\ ^{C^{d_m}})\ mod\ p$.

inc th scro a thoriti s do not r al th al s C^{d_i}, no on can r co r x. or proofs of s c rit r f r th r ad r to [YY99].

6 pt - scr i rarc

h last sol tion can b combin d ith [YY9] to impl m nt a d pth-3 scro hi rarch . h follo ing is ho to r ali s ch a s st m. h scro a thoriti s g n rat a shar d composit n s ch that $q = 2tn +$ is prim , and s ch that $p = 2q +$ is prim . H r t is a small prim of th form $2t +$ h r t is prim . h s, from th root of th tr to th childr n of th root, th scro s st m that is s d is th on that is d scrib d in this s ction. It is som hat mor diffic lt to g n rat an appropriat prim $2tn+$ in this cas , sinc $4tn+3$ m st also b prim (so ha th sam in ffici nc as in [YY9]). ach child of th root (int rm diat nod) th n g n rat s a (pot ntiall shar d) p blic k Y *mod* $2q$. h s Y is an l amal p blic k in l amal mod $2q$.

h l a s corr sponding to (i. . nd r) ach of th s int rm diat childr n th n g n rat scro d k s bas d on th al s for Y sing th algorithm from [YY9]. h s, th [YY9] algorithm is s d b t n th int rm diat nod s and th s rs at th l a s. ot that in this cas th g n rator that is s d in Y ma onl g n rat a larg s bgro p of Z_q .

7 c t l p ts

h r ar a n mb r of things that co ld impro on th s to- co rabl to- rti abl cr ptos st ms. or instanc , it is d sirabl to liminat th ass mption that robl m and robl m 2 ar hard. lso, not that in both s st ms, th s r's p blic k s ha sp cial alg braic form, as dictat d b th ir r lianc on th shar d p blic k of th scro a thoriti s. In a g n ric s st m on o ld lik to b abl to scro g n ric k s (and r g lar l- amal). his gi s ris to th follo ing additional r q ir m nts.

9. **pl i g ri K s** h s st ms s th traditional p blic k s: /factoring-bas d or l amal ariants.
2 . **patibl s r** h onl chang for th s r is additional information s nt d ring k r gistration (or r r gistration).
2 . **as adi g a g s** h s rs do not ha to chang th ir applications hich mplo cr ptograph , not n ithin th KI applications (nam l th s th sam g n ral cr ptographic f nctions, and th sam soft ar , all chang is som add d proc d r in r gistration).
22. **p rati s rs a d s r g ts** h scro a thoriti s ar manag d and constr ct d ind p nd ntl of th s rs (onl th ir p blic k (s) n d b kno n).
23. **I d p d t s r K s** h s r's k is ind p nd nt of an third part k and is prod c d in m ch th sam a as in an n scro d KI. h s rs can k p th ir basic cr ptographic algorithms (k g n ration, ncr ption, tc.).
24. **ltipl s r t riti s** s rs can r gist r for scro ith m ltipl scro a thoriti s.

25. **ist s r / - s r** s rs can nd r th sam ha n scro d k s and scro d on s (and can transf r n scro d k s to scro d on s).
26. **s r i rar** m lti-l l s c rit s st m can b impl m nt d h r scro a thoriti s at ach l l can acc ss all information b lo in th hi rarch , and non of th information abo .

rt c i r

In ork that is t to app ar, pr s nt an to- co rabl to- rti abl cr ptos t m ith l amal s r k s that do s not in ol an n cr ptographic ass mptions (lik robl m or robl m 2 b ing hard). In fact, all that is ass m d is th ist nc of a s manticall s c r K (tho gh th random oracl mod l is still s d). H nc , th shar d p blic k of th scro a thorit can ha an alg braic form, so long as it is part of a s manticall s c r K . h sol tion d co pl s th alg braic conn ction b t n th s r k s and th shar d p blic k of th scro a thorit , and th s gi s ris to a compl t l n f at r in to- co rabl to- rti abl cr ptos st ms. It nabl s "drop-in r plac m nt" of c rti d p blic k s. his r s lts from th fact that th p blic k of th s r can b g n rat d in *actl* th sam a as in an n scro d KI. h s, sho ld a s r n d cid to scro his or h r p blic k , h or sh can do so at an tim , n aft r th p blic k is mad p blic. h s r n d onl constr ct th c rti cat of r co rabilit at a lat r tim and s bmit it for ri cation b th . In f t r ork ill b pr s nting s ch a s st m h r th s r's p blic k is an p blic k [YY-ms]. his d co pling of th alg - bra b hind th p blic k s also nabl s arbitrar d pth k scro hi rarchi s. h n s st ms ha th prop rti s sp ci d abo .

f r c s

e a e, S a e e fiab e Pa a e E c
,

D eh, a Effic e e e a f Sha e RS e *dv n s in g Y '* , S ge - e ag

DD Y 4 De Sa , Y De e , Y a e , Y g Sha e a c Sec e S The f g, age 5 5 , 4

D D ffie, e a e D ec g a h e T- , f EEE T a ac f a The , age 44 54,

E 85 T E a a P b c- e e a a S g a e Sche e a e D c e e ga h RYPT 84, age 8

D8 Y a e , Y De e Th e h e RYPT 8 , age - 5

S8 a , Sha P e Y e f P ac ca S e fica a S g a e P b e RYPT 8 , age 8 4

Y 5 Y a e, Y g E c E c S e e ac , a a De g RYPT 5, age 5,

Y Y a e, Y g cha ac e a f E c E c Sche e P
Y85 Z a , S abe , Y g S e c b c- e e c RYPT 85, age 8 85
-S be , R e , S e , e a h, a e, D ffie, - e, P e a , R R e , Sch e , Sch e e The R f e Rec e , e E c , a T e Th -Pa E c a a ab e a h c c e _
5 a a T e gh a e Re e RYPT 5, age 8 , 5 S ge - e ag
h 8 h fe e e h f e fica T ab f e Sc e ce, a b ge a , a 8
Y 5 e a, P e , Y Yac b e E c S e h a a RYPT 5, age , 5
S ca a P b c- e e RYPT , age 8, S ge - e ag
P Pfi a , a e ea a -De ec ab e e E c E c e
R R R e E e e a be The a ca e , The e 8 4, age 5, e e
S S a e P b c e fiab e Sec e Sha g E c , age , S ge - e ag
T T e a U b g E a a - e a e e -e c E c e
T E e he , a T b g g E a a a -De ec ab e e a e e -E c P a E c , age ,
YY Y g, Y g The Da S e f ac - g a h RYPT , age 8 ,
YY a Y g, Y g e g a h U g g a h aga g a- h E c , age 4
YY b Y g, Y g The P e a e ce f e g a h c ac D c e e- g a e e RYPT , age 4 S ge - e ag
YY 8 Y g, Y g -Rec e ab e a - e fiab e e *dv n s in g* ,
YY Y g, Y g -Rec e ab e e h a e a a- a The E c e a ch ,
YY- Y g, Y g a c a a ab e f a h

A Distributed Intrusion Detection System Based on Bayesian Alarm Networks

Dusan Bulatovic[1] and Dusan Velasevic[2]

[1] Informatika, Jevrejska 32,
11000 Belgrade, Yugoslavia
dusanb@informatika.com
[2] University of Belgrade, School of Electrical Engineering,
11000 Belgrade, Yugoslavia
velasevic@buef31.etf.bg.ac.yu

Abstract. Intrusion Detection in large network must rely on use of many distributed agents instead to one large monolithic module. Agents should have some kind of artificial intelligence in order to cope successfully with different intrusion problems. In this paper, we suggested Bayesian alarm network to work as independent Network Intrusion Detection Agent. We have shown that when narrowed in detecting one specific type of the attack in large network, for example denial of service, virus, worm or privacy attack, we can induce much more prior knowledge into system regarding the attack. Different nodes of the network can develop their own model of Bayesian alarm network and agents could communicate between themselves and with common security data base. Networks should be organized hierarchically so on the higher level of hierarchy, Bayesian alarm network, thanks to interconnections with lower level networks and data, acts as a distributed Intrusion Detection System.

1 Introduction

Due to increased connectivity (especially on the Internet), and the vast of financial possibilities that are opening up in electronic trade, more and more computer networks and hosts are subject to attack. One way to prevent subversion is by building a completely secure system. However this is not possible in practice. The vast installed base of systems world-wide, guarantees that any transition to a secure system and network, if ever attempted, would take long time in coming.

It seems obvious that we cannot prevent subversion. Tools are therefore necessary to monitor systems, to detect attacks, and to respond actively to them. This is essentially what is expected from one Intrusion Detection System (IDS) to be able to do.

An intrusion is defined [1] as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. It is a violation of the security policy of the system. Any definition of an intrusion is, of necessity, imprecise, as security policy requirements do not always translate into a well defined set of actions. From the other side, Intrusion Detection is the methodology by which intrusions are detected. This methodology can be divided into two category of intrusion, *misuse* intrusion and *anomaly* intrusion that can be described as:

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 219–228, 1999.

- Misuse intrusions are well defined attacks on known weak points of a system. They can be spotted by watching for certain actions being performed on certain objects.
- Anomaly intrusions are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.

As misuse intrusions follow well-defined patterns they can be detected by doing pattern matching on audit- trail information. However, anomaly intrusions are harder to detect. There are no fixed patterns that can be monitored for and so we need a system that combined human-like pattern matching capabilities with the vigilance of a computer program. Thus it would always be monitoring the system for potential intrusions, but would be able to ignore spurious false intrusions if they resulted from legitimate user actions; so another goal is to minimize the probability of incorrect classification.

In large networks, Intrusion Detection Systems must relay on network wide information. Often, use of many distributed agents instead of one large monolithic IDS module will give better results. Agents should have some kind of artificial intelligence in order to cope successfully with different intrusion problems. As a future direction in developing IDS, it is believed that Bayesian network should be used. In a general case it is not clear how to do that, but we will show that when narrowed in detecting one specific type of the attack, for example denial of service, virus, worm or privacy attack, we can induce much more prior knowledge into the system regarding the attack.

Before we present our solution, we will first describe three corresponding methods of network intrusion detection.

2 Use of Genetic Programming in Intrusion Detection

Many seemingly different problems in artificial intelligence, can be viewed as requiring discovery of a computer program that produces some desired output for particular inputs. When viewed in this way, the process of solving these problems becomes equivalent to searching a space of possible computer programs for a most fit individual computer program.

This approach is chosen in [2] to building IDS. Instead of one large monolithic IDS module, here is used a finer-grained approach with a group of free-running processes which can act independently of each other and the system. They are called Autonomous Agents.

An agent is defined as [3] a system that tries to fulfill a set of goals in a complex, dynamic environment. In this context, every agent would try to detect anomalous intrusions in a computer system under continually changing conditions. In other words, the agent would be the IDS. If an IDS can be split up into multiple functional entities which can operate in their own right, each of them can be an agent. This gives multiple intrusion detection systems running simultaneously. The agents run in parallel in the system. Each agent is a lightweight program - it observes only one small aspect of the overall system. A single agent alone cannot form an effective intrusion detection system - its view of the overall system is too limited in scope. However, if

many agents all operate on a system, then a more complicated IDS can be built. Agents are independent of each other. They can be added to and removed from the system dynamically.

The agent code is composed of a set of operators (arithmetic, logical and conditional) and a set of primitives that obtain the value of metrics. As is usual with Genetic Programming, these sets can be combined in any way during evaluation run to generate parse trees for solution programs.

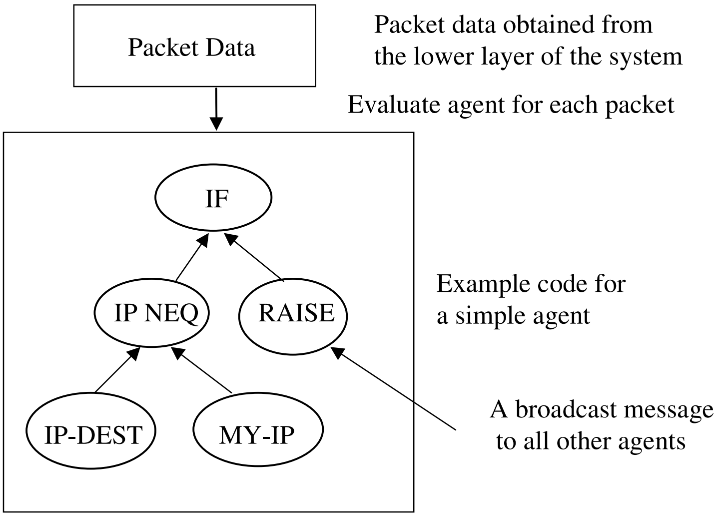


Fig. 1: Sample internal parse tree for an agent

Figure 1 shows a sample parse tree for an agent. The Terminals in the parse tree (the primitives IP-DEST, MY-IP and RAISE) obtain their values from the system abstraction layer. In this simple example, the primitive IP-DEST would obtain the IP Destination address for the current packet from the abstraction layer.

The advantages of using genetic programming looked trough the model of Autonomous agent are efficiency, fault tolerance, resilience to degradation, extensibility and scalability. Having many small agents has a number of advantages against a single monolithic IDS. Clear analogy can be drawn between the human immune system and this proposal. The immune system consists of many white blood cells dispersed throughout the body. They must attack anything which they consider to be alien before it poses a threat to the body.

The foreseen drawbacks include the overhead both on hosts and network because of so many processes, long training times, and the fact that if the system is subverted, it becomes a security liability. An interesting possibility they open up is that of an active defense, that can respond to intrusions actively instead of passively reporting them (it could kill suspicious connections, for example). Developing good training scenarios is an important issue with this model and that should be area for future investigation.

3 Graph Based Intrusion Detection

This approach in Intrusion Detection will be described on the model developed by group of authors in University of California, Davis [4]. Their work was inspired by Internet Worm Attack (1988), which caused the Internet to be unavailable for about five days [5]. They designed GrIDS - Graph-based Intrusion Detection System in order to develop secure infrastructure capable to defend Internet and other large networks. Its primary function is to detect and analyze large-scale attacks, although it also has the capability of detecting intrusions on individual hosts.

The nature of operation of the GrIDS system will be presented on a simple example of tracking warm and building such an activity graph.

In Figure 2 the worm begins on host A, then initiates connections to hosts B and C which causes them to be infected. The two connections are reported to GrIDS, which creates a new graph representing this activity and records when it occurred. The two connections are placed in the same graph because they are assumed to be related. In this case, this is because they overlap in the network topology and occur closely together in time.

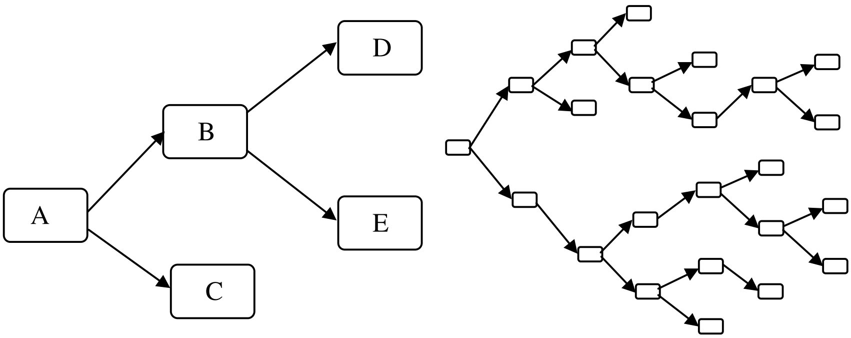


Fig. 2: The beginning of a worm graph, and the graph after the worm has spread

If enough time passes without further activity from hosts A, B, or C, then the graph will be discarded. However, if the worm spreads quickly to hosts D and E, as in the figure, then this new activity is added to the graph and the graph's time stamp is updated.

Graph-based Intrusion Detection is a helpful step toward defending against widespread attack in the networks. It presents network activities to humans as highly comprehensible graphs. In addition, policy mechanisms allow organizations much greater control over the use of their networks than is possible, for example, with firewalls alone.

GrIDS, implementation of the graph-based Intrusion Detection, is designed to detect large-scale attacks or violations of an explicit policy. However, a widespread attack that progresses slowly will not be diagnosed by its aggregation mechanism.
Also additional safeguards must be taken to ensure the integrity of communications between GrIDS modules, and to prevent an attacker from replacing parts of GrIDS with malicious software of her own.

4 Cooperative Intrusion Detection for Detecting Denial of Network Service

Denial of service for the routing infrastructures, (routers and routing protocols), may be caused by natural faults as well as by malicious attacks. To protect network infrastructures from routers that incorrectly drop packets and misroute packets, Cheung and Levitt [7] used a detection - response approach. They presented protocols that detect and respond to those misbehaving routers.

Protocols are supposed to detect and respond to two types of denial of service, "black hole" routers and routers that misroute packets.

One of the proposed protocols, *distributed probing* is applicable to detecting network sinks and misrouting routers that cause denial of service - that is, the misrouted packets cannot reach their destinations. With distributed probing, a router can diagnose its neighboring routers by sending them directly (i.e., without passing through intermediate routers) a test packet whose destination router is the tester itself. Based on whether a tester can get back the test packet within a certain time interval, the tester can deduce the goodness of the tested router.

Network is modeled by a directed graph $G = (V;E)$ where vertices denote routers and edges denote communication channels. An edge $(i; j) \in E$ is called testable if $cost(j; i)$ is strictly less than the cost of any other path from j to i in G, where the cost of a path is the sum of the costs of all edges on the path. In Figure 3 we have a network example that has three routers, namely a, b, and $\boldsymbol{c}$. and three edges (b,c), (b,a), and (c,b). If (c,b) is testable and router c sends a packet p whose destination is c itself to b, then, in distributing probing protocol, p will return to c if and only if b does not misbehave on p.

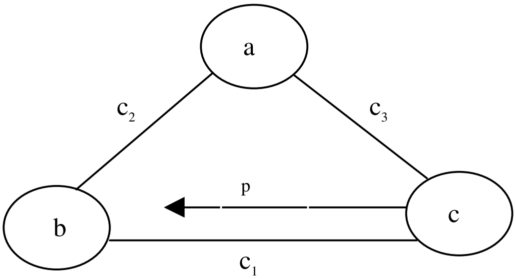


Fig. 3: Testable edges

This model of cooperative work for detecting denial of service, unfortunately, does not solve the entire denial of service problem of routing infrastructures. There are router failures not covered by this failure models. For example, a compromised router may modify the body of a transit packet. Also, link failures are not modeled, so a link failure that results in packet loss may be viewed as a node failure. Finally, these models only consider transit traffic. In other words, packets sent by source hosts to source routers and those sent by destination routers to destination hosts are not addressed. However, this model represent a first step in protecting routing infrastructures from denial of service using an intrusion detection approach.

5 Our Proposal: A Bayesian Alarm Network as Independent Intrusion Detection Agent

Bayesian approach to probability and statistics differs from the classical probability. Whereas a classical probability is a physical property of the world (e.g., the probability that a coin will land heads), a Bayesian probability is a person's degree of belief in that event.

Important difference between physical probability and personal probability is that, to measure the latter, we do not need repeated trials. While classical statistician has a hard time measuring that the cube will lend with a particular face up, the Bayesian simply restrict his attention to the next toss, and assigns a probability.

For some events it is not possible to measure the probability and that is why Bayesian classification represents interesting tool in intrusion detection. This technique of unsupervised classification of data, and its implementation, Autoclass [8] searches for classes in the given data using Bayesian statistical techniques. It attempts to determine the most likely process(es) that generated the data. It does not partition the given data into classes but defines a probabilistic membership function of each datum in the most likely determined classes.

Bayes' rule does not provide an algorithm for classification. The designers of a Bayesian classifier are faced with the computationally intractable problem of searching the hypothesis space for the optimal distribution that produced the observed data and the controversial problem of estimating the priors.

In the case where we are faced with large number of variables and relationships among them Bayesian network is a representation suited to solve the problem. It is a graphical model (directed acyclic graph-DAG), that can efficiently encode the joint probability distribution (physical or Bayesian) for a larger set of variables.

The idea to use Bayesian or other belief networks in Intrusion Detection Systems has come from the necessity to combine different anomaly measures in detecting intrusions. Bayesian networks [10] allow the representation of causal dependencies between random variables in graphical form and permit the calculation of the joint probability distribution of the random variables by specifying only a small set of probabilities, relating only to neighboring nodes. This set consists of the prior probabilities of all the root nodes (nodes without parents) and the conditional probabilities of all the non root nodes given all possible combinations of their direct predecessors.

Bayesian networks, which are DAGs with arcs representing causal dependence between the parent and the child, permit absorption of evidence when the values of some random variables become known, and provide a computational framework for determining the conditional values of the remaining random variables, given the evidence. Figure 4 gives a trivial Bayesian network modeling intrusive activity.

Each box represents a binary random variable with values representing either its normal or abnormal condition. If we can observe the values of some of these variables, we can use Bayesian network calculus to determine P(Intrusion|Evidence).

However, to determine the a priori probability values of the root nodes and the link matrices for each directed arc for a general case, where many different intrusion are possible, we must incorporate a substantial amount of knowledge concerning the different types of attacks that can be used to compromise system security, as well as the conditional probabilities that various well-defined events will occur given that

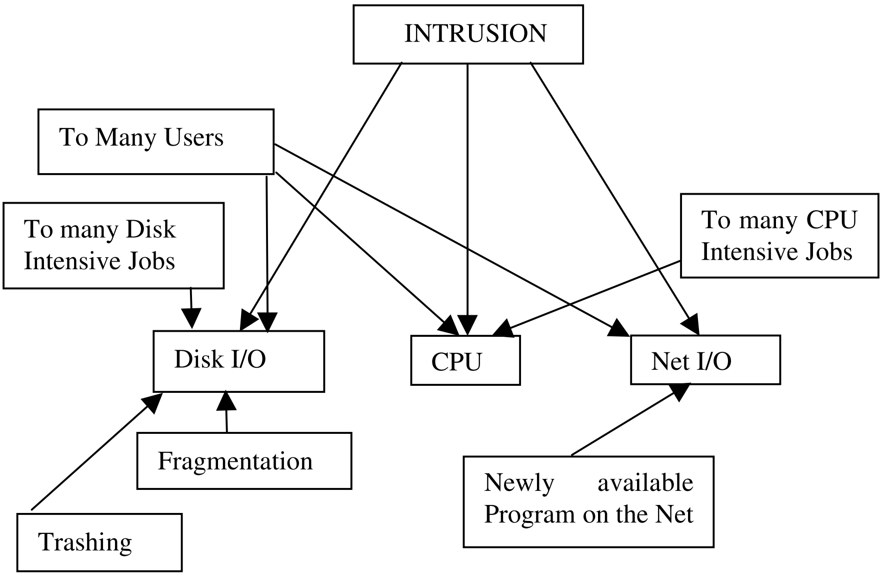


Fig. 4: Bayesian alarm network – general case

those attacks are in progress. Unfortunately, Intrusion-detection community is at the moment only at first stage of trying to assemble this type of knowledge.

Our proposal is, because of complicity to find general solution, not to use Bayesian alarm network as universal, standalone Intrusion Detection System. Instead, it could be used as independent Intrusion Detection Agent for detecting one, *specific* type of network attack. This way we need to induce into the system prior knowledge only regarding that type of the attack. At the same time some other nodes of large network can develop its own model of alarm network for detecting same kind of the attack, entering freely local believes in data sensitivity, and expectation of the attack. These agents should be able to communicate between themselves on broadcast or search principle, as required.

Beside being able to communicate between themselves, this approach require for agents to communicate with a common data base-Bayesian Management Information Base (BMIB), which contains information regarding the attacks in progress. However, different site will normally select different vendors and, since network incidents are often distributed over multiple sites, it is likely that a single incident will be visible in different way.

Clearly, it would be necessary for these diverse intrusion detection systems to be able to share data. Solution to that problem could result from the work of a new Intrusion Detection working group established in the Security Area of the IETF to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and the management systems which have to interact with them.

However, for our model, not only data format in BMIBs and exchange procedure must be standardized, but also notation of the network attacks, like P–for privacy, V-for virus , W-for worm, D-for denial of service etc.

For the definition of the architectural model that could be used in the implementation of the security management system, hierarchical organization of the networks and BMIBs is suggested [12]. The lower level of the hierarchy should include a small number of interconnected physical networks. Network of the upper level will interconnect the lower levels networks and BMIB will contain relevant information regarding attacks in wider area.

Due to sophisticate nature of network attacks the security management cannot rely only on the real-time monitoring of security measures. The network manager needs also to store in a database and analyze historical security information in order to detect an attack as a symptom of past correlated events and to discover the attacker.

As an illustration of solving the specific problem of detecting privacy attack to sensitive medical records, in Figure 5 is given a simplified structure of a corresponding Bayesian alarm network. One possible choice of variables for this problem was Intrusion (I), Aids (A), External (E), Medical (M), Nonmedical (N), Outsider (O), where I represent that current access to sensitive records is intrusion to privacy, A - access to records with diagnose of aids and E access to external sensitive records (other ward or hospital). Variables M, N and O denote that access is performed by medical staff, nonmedical staff, or outsider.

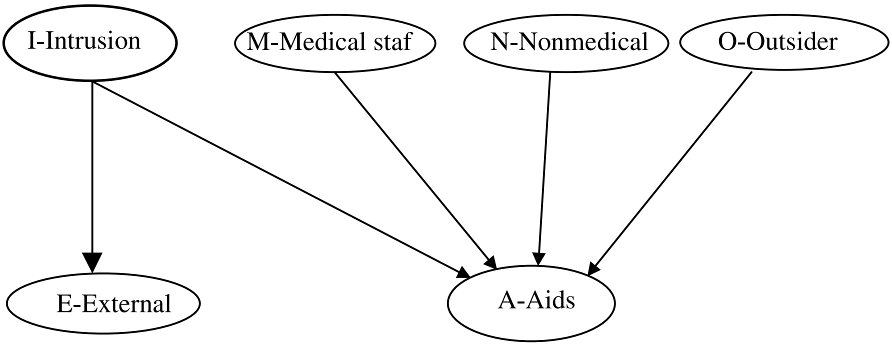


Fig. 5: One specific attack (privacy intrusion) - simpler Bayesian alarm network

In this example, using ordering (I,M,N,O,E,A) we have the following conditional independencies:

$$p(m|i) = p(m) \ ,$$

$$p(n|i,m) = p(n) \ ,$$

$$p(o|i,m,n) = p(o) \ ,$$

$$p(e|i,m,n,o) = p(e|i) \ ,$$

$$p(a|i,m,n,o,e) = p(a|i,m,n,o) \ . \tag{1}$$

As seen, we consider that accesses to sensitive records at different places are conditionally independent. Also, accesses by medical staff, nonmedical or outsider are mutually conditionally independent. Our judgments about conditional independence between various variables, guide us to the network structure where it is possible easier to compute the probability of interest (probability of intrusion):

$$p(i|m,n,o,e,a) = \frac{p(i,m,n,o,e,a)}{p(m,n,o,e,a)} = \frac{p(i,m,n,o,e,a)}{\sum_{i'} p(i',m,n,o,e,a)} \ . \tag{2}$$

Given the conditional independencies in Equation (1), we can make this computation more efficient:

$$p(i|m,n,o,e,a) = \frac{p(i)p(m)p(n)p(o)p(e|i)p(a|i,m,n,o)}{\sum_{i'} p(i')p(m)p(n)p(o)p(e|i')p(a|i',m,n,o)} \tag{3}$$

i.e.:

$$p(i|m,n,o,e,a) = \frac{p(i)p(e|i)p(a|i,m,n,o)}{\sum_{i'} p(i')p(e|i')p(a|i',m,n,o)} \ . \tag{4}$$

From the presented example it is also possible to conclude that requirement for the prior knowledge regarding the attack is not drawback in the case of Bayesian network developed to detect one specific kind of intrusion. As we are here concentrated to one type or a small subset of intrusions, it is expected that we should have more knowledge regarding the matter. At the same time thanks to interconnections with other alarm networks at the same level of hierarchy and corresponding BMIB we should be able to collect more knowledge and data regarding the same type of the attack. (Connection to other alarm networks is here symbolically denoted with variable E – access to external sensitive records in other ward or hospital).

At higher level of hierarchy, based to its interconnections with lower level networks and data from Bayesian Management Information Base, Bayesian alarm network will be able to monitor network attacks in wider area, and can act as *Distributed Intrusion Detection System*. Using recorded data from BMIBs such a distributed Intrusion Detection System, with assembled knowledge from different Bayesian alarm networks, could have integrated, human and computer program intrusion detection capability.

6 Discussion

It is shown that our model will provide Bayesian alarm network to work as independent Intrusion Detection System, and, at the same time, to be part of a larger distributed IDS.

In opposed to others agents based Intrusion Detection, our agent do not have limited capability but can work as standalone IDS. Different sites, with different vendors selected, can develop independently its own model of alarm network for detecting same kind of the attack, but agents will be able to communicate between themselves thanks to standard data format, exchange procedure and notation of the attacks.

Beside standardization in messaging, in our approach is as well important introduction of Bayesian Management Information Base (BMIB) concept. BMIB will store information regarding the attack in progress and also historical security information. Based on hierarchical organization of networks, it is possible to develop distributed Intrusion Detection System that will use information from BMIBs and communicate with lower lever networks.

With Bayesian alarm network in conjunction with Bayesian statistical techniques, we can easy overcome problem of missing data and facilitate the combination of prior knowledge and data especially in the case, (what is usual with Intrusion Detection), when no experiments are available. Finally with Bayesian alarm network we have no problem with different type of data as different type of attributes may be freely mixed.

Bayesian alarm network in described framework can be used not only to detect intrusion but to play active role in protecting networks as well. Due to nature of Bayesian probability it could be able to prevent on going attack even if we have not evidenced that kind of attack before.

References

1. R. Heady, G. Luger, A. Maccabe, and M. Servilla. The Architecture of a Network Level Intrusion Detection System. Technical report, University of NewMexico, Department of ComputerScience, August 1990.
2. Crosbie M., October 1995. Defending a Computer System using Autonomous Agents. In Proceedings of the 18th NISSC Conference, October 1995.
3. Maes P. 1993. Modeling adaptive autonomous agents.Artificial Life 1(1/2).
4. S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS -- A Graph-Based Intrusion Detection System for Large Networks". The 19th National Information Systems Security Conference, 1996.
5. M. Eichin and J. Rochis. With microscope and tweezers: An analysis of the Internet worm of November 1988. IEEE Symposium on Research in Security and Privacy, 1989.
6. D. Seely. A tour of the worm. IEEE Trans. On Soft. Eng., November 1991.
7. S. Cheung, K. N. Levit: Protecting Routing Infrastructure from Denial of Service Using Cooperative intrusion Detection. In Proceedings of New Security Paradigm Workshop, Cumbria, UK, September 1997.
8. P. Cheeseman, J. Stutz, and R. Hanson: Bayesian classification with correlation and inheritance. Proceedings of 12th International Joint Conference On Artificial Intelligence pages 692-698, San Mateo, California, 1991.
9. K. Fukunaga. Introduction to Statistical Pattern Recognition. Academic press, New York, 1990.
10. D. Heckerman, Probabilistic Similarity Networks. MIT Press, 1991.
11. G. Finn, “Reducing the Vulnerability of Dynamic Computer Networks," ISI Research Report RR-88-201, University of Southern California, June 1988.
12. T. Apostolopoulos,V. Daskalou: “On the implementation of a Prototype for Performance Management Services”, Proceedings of IEEE Int Symp. on Computers and Communications, ISCC’95, 1995.
13. D. Comer, “Internetworking with TCP/IP." Vol.1, Prentice Hall, 1991.
14. R. Perlman, “Interconnections: Bridges and Routers." Addison-Wesley, 1992.
15. Biswanath Mukherjee, L Todd Heberlein and Karl N Levitt. Network Intrusion Detection, IEEE Network, May/June 1994, pages 26-41.

Interoperability Characteristics of S/MIME Products

Sarbari Gupta[1], Jerry Mulvenna[2], Srinivas Ganta[1], Larry Keys[2], and Dale Walters[2]

[1]CygnaCom Solutions, Inc., 7927 Jones Branch Drive Suite 100W, McLean, VA
{sgupta, sganta}@cygnacom.com
[2]National Institute of Standards and Technology, Gaithersburg, MD
{mulvenna, keys, walters }@csmes.ncsl.nist.gov

Abstract. S/MIME is based upon the popular MIME standard, and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The S/MIME version 2 specification was designed to promote interoperable secure electronic mail. However, because the specification allows multiple interpretations and implementations, and is sometimes silent about key aspects that affect interoperability, a number of "S/MIME Enabled" products are available on the market that are incapable of fully interacting with one another. In this paper, we present a set of characteristics that affect the interoperability profile for a given S/MIME application, and illustrate how they may be used to achieve a higher level of interoperability within the family of S/MIME compliant products. We also analyze the S/MIME version 3 specification to determine what subset of the identified interoperability characteristics still remain to be adequately addressed.

1 Introduction

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a specification for securing electronic mail. S/MIME is based upon the popular MIME standard, and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The exact security services offered by S/MIME are authentication, non-repudiation, message integrity, and message privacy.

The S/MIME Version 2 specifications were designed to promote interoperable secure electronic mail, such that two compliant implementations would be able to communicate securely with one another [6, 7]. However, because the specification allows multiple interpretations and implementations, and is sometimes silent about key aspects that affect interoperability, what has resulted is the availability of multiple S/MIME compliant commercial products that are not capable of fully interoperating with one another with respect to secure messaging.

Recently, the S/MIME Version 3 specifications were passed by the IESG (Internet Engineering Steering Group) and are in the process of being published as RFC (Request For Comment) standards by the IETF (Internet Engineering Task Force) [8, 9]. However, this paper describes the findings of a set of interoperability experiments that were conducted using commercial-off-the-shelf (COTS) S/MIME version 2 products from different vendors. The experiments were

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 229–241, 1999.

designed to test the interoperability between peer S/MIME applications, between S/MIME applications and Certification Authority products, and between S/MIME applications and Directories. Other groups have also conducted tests on S/MIME applications and have published results [10].

All of the S/MIME implementations tested have been awarded the "S/MIME Enabled" seal based upon compliance tests conducted by RSA Labs. [Appendix A lists the actual products that were used in the tests.] Yet, there were a significant number of scenarios, where interoperability between the implementations was either limited or unachievable. From the test results, we concluded that there are a number of characteristics or properties that affect the interoperability of a given S/MIME application with other S/MIME applications, Certification Authority products and Directory products. These characteristics are neither part of the S/MIME version 2 specifications, nor do they appear in the S/MIME compliance testing methodology adopted by RSA. The recently approved S/MIME version 3 standard addresses some, but not all of the characteristics described in this paper.

In this paper, we discuss these characteristics and illustrate how they affect the interoperability profile for a given S/MIME application. Interoperability is a prime concern of users of S/MIME implementations. Awareness of these characteristics may help to fine tune the S/MIME specifications to support a greater level of interoperability. They may also help the developers of S/MIME applications to make design decisions that would further the cause of interoperability. Additionally, these characteristics may help individuals who are procuring S/MIME applications to differentiate between the available implementations and select the one that most closely meets their interoperability needs. Finally, although these characteristics were derived from tests conducted upon S/MIME implementations, they may be applied to any end-user security application that requires a public key infrastructure.

The rest of this paper is organized as follows. Section 2 describes the necessary background including the evolution and current status of the S/MIME specification. Section 3 describes a categorized set of characteristics that impact the ability of an S/MIME implementation to interoperate with other implementations. Section 4 discusses how the findings in this paper can be used to attain a higher level of awareness about the potential bottlenecks to interoperability. Section 5 analyzes the S/MIME version 3 specifications to identify the S/MIME interoperability characteristics that have been adequately addressed, and the ones that still need more attention at the specification level. Finally, our conclusions are presented in Section 6.

2 Background

2.1 Evolution of the S/MIME Standard

The Multipurpose Internet Mail Extension (MIME) was also developed by the IETF, and was designed to support non-textual data (such as graphics data or video data) as the content of an Internet message [4,5]. Additional structure was imposed on the MIME message body to provide an encryption and digital signature service as part of the S/MIME specification.

2.2 S/MIME Version 2

The S/MIME specification uses data structures that conform to Public Key Cryptographic Standard (PKCS) #7 [1]. PKCS #7 is a cryptographic message syntax that is designed to specify the content and form of the information that is required in order to provide an encryption and digital signature service.

S/MIME implementations support several different symmetric content encryption algorithms. The RC2 algorithm with a key size of 40 bits is supported, even though it provides weak encryption, in order to comply with U.S. export regulations. In addition, in most S/MIME implementations, the user can choose DES, Triple DES or RC2 with a key size greater than 40 as the content encryption algorithm. The user can normally select either SHA-1 or MD5 as the message digest algorithm; the receiver's application must be able to process both algorithms. The sender's system must use the RSA public key algorithm with a key size ranging from 512 to 1024 bits to sign a message digest or to encrypt the content encrypting key

A Certification Authority (CA) issues certificates that bind the identity of a public key to a user. This binding is only as strong as the out-of-band verification that the CA performs before issuing the certificate. Since many CAs can issue certificates, there must be a method of establishing trust among CAs so that each user can trust the information in a certificate issued by a CA other than his own. After the public certificate is issued, there must be a method by which the certificate is made available to other users. The certificate must be in a standard format so that the information in the certificate can be processed by applications built by different vendors.

Deployment of S/MIME secure e-mail implementations requires a supporting Public Key Infrastructure (PKI) to provide solutions for the issues listed above. In some cases, standards have already been developed and implemented to provide this infrastructure. There is agreement that the certificate format will conform to Version 3 of the International Telecommunications Union (ITU) x.509 Recommendations. There is agreement that the Lightweight Directory Access Protocol (LDAP) is the protocol that will be used to access the directories that function as certificate repositories. PKCS#10 specifies the format for a request for a CA to issue a certificate [2].

2.3 S/MIME Version 3

The S/MIME Version 3 specification [8, 9] is based on the usage of data structures from the Cryptographic Message Syntax (CMS) published as an RFC [11] by the IETF. CMS is derived from PKCS#7 version 1.5. The changes were designed to accommodate key agreement techniques for key management and the support of attribute certificates.

Version 3 products are mandated to support the use of DSA (Digital Signature Algorithm) for signatures, and DH (Diffie-Hellman) for key establishment. The use of RSA for signature and key exchange is not mandated, but is specified as desirable. The symmetric encryption algorithm that must be supported by all Version 3 implementations is Triple DES (DES EDE3 CBC). 40 bit RC2 is supported as a non-mandatory algorithm to allow backward compatibility with Version 2 implementations.

Version 3 specifies a number of attributes that may be sent within the CMS message as either signed or unsigned attributes. Receiving agents must be able to process these attributes. The signed attributes that may be included in a Version 3 message are, signing time, S/MIME capabilities, S/MIME encryption key preference, and signing certificate. It may be noted that the Version 3 specification implicitly supports the usage of separate key pairs (and hence certificates) for signature and key exchange.

The S/MIME capabilities signed attribute allows the sender to specify their algorithmic preferences in the order of preference. This allows a peer to select the algorithms that are appropriate. Both opaque as well as multipart formats are supported for signed messages in Version 3, but neither one is specified as being mandatory for sending or receiving agents. The support for messages that carry only certificates to the peer is supported in Version 3, thus allowing in-band certificate distribution.

Certificates and certificate revocation lists used within Version 3 implementations must be compliant with [1]. Receiving agents must validate peer certificates (including revocation checking) for all messages. Version 3 also supports the use of X.509 attribute certificates. Receiving agents must be able to handle messages that contain no certificates using a database or directory lookup scheme.

2.4 S/MIME Compliance Tests from RSA

S/MIME products are being developed to interoperate with the products of different vendors. When they purchase an S/MIME product, users want to know that they can exchange signed and encrypted messages with any other S/MIME user. RSA Data Security has set up an S/MIME Interoperability Center that allows vendors to perform interoperability testing on their products and to have the results published.

The RSA Interoperability Test Center was established in 1997. Participating vendors test against WorldTalk's WorldSecure Client which is the designated reference implementation. All vendors participating in the testing use Verisign's Class 1 public key certificates. The vendor first sends a signed message containing a public key certificate to the reference implementation and receives two signed and encrypted messages in return. One message uses RC2 as the content encryption algorithm; the second message uses Triple-DES for content encryption. Both messages contain a secret phrase. The vendor decrypts the messages, extracts the secret phrases and includes them in the messages sent back to the reference implementation, using the same content encryption algorithm. If the reference implementation can recover the secret phrases, the successful test results will be posted on the S/MIME Interoperability Test Center Web Page (www.rsa.com/smime). As of January 1999, more than 20 different S/MIME products have been successfully tested. [Appendix B lists the products that have been awarded the S/MIME compliance seal by RSA Labs.]

The testing, while providing useful information is limited in scope. It doesn't test the ability of an S/MIME implementation to interact with a certificate repository in order to publish or obtain a public key certificate. It doesn't test the ability to process certificates issued by different Certification Authorities or the ability to process Certification Revocation Lists. It also doesn't follow that, because the

implementations test successfully with the reference implementation, they will successfully test with each other.

3 Interoperability Characteristics

This section describes characteristics and properties that are pertinent to the ability of an S/MIME implementation to interoperate with peer implementations, Certificate Authorities, and Repositories. The properties are categorized into sets that affect a particular area of operation of a specific implementation.

3.1 Certificate Handling

This section describes characteristics related to the management and use of certificates within an S/MIME implementation.

Managing Certificates for Local User. The local user is the human entity that controls an S/MIME application to send and receive secure email with its peer entities.

Distinct Signing and Encryption Certificates for Local User. The S/MIME Version 2 specification calls for the use of a single certificate for signing outgoing email as well as receiving incoming encrypted email. Most currently available S/MIME implementations support a single certificate for the local user running the S/MIME application. S/MIME Version 3, however, supports the use of separate certificates for signatures and encryption, and a small set of S/MIME implementations implement this two-certificate scheme [8, 9].

An S/MIME application that only supports a single certificate for encryption and signatures may be unable to communicate securely with a peer that supports a dual certificate scheme. For example, a typical S/MIME implementation will try to use the certificate used to validate a signed message from a peer to send encrypted message to that peer entity. However, if the peer happens to be a dual-certificate-based implementation, it will reject the incoming encrypted message since it will not be able to use its own encryption certificate to decrypt the message. Thus, single certificate implementations provide the greatest level of interoperability in the current S/MIME version 2 space of products. If dual-certificate implementations are used, it is recommended that users identify the same certificate as the signature as well as the encryption certificate.

Self-Signed Certificate Support for Local User. The use of the security features of S/MIME within a group of peer entities is predicated upon the availability of a PKI that allows an entity within the group to establish trust in the public key certificates of every other entity within the group. However, the deployment of large-scale public key infrastructures has been neither easy nor widespread. In the absence of a PKI, certain trust models allow a small group of peers to trust one another implicitly. This is typically achieved by exchanging certificates via some secure means and trusting

peer certificates implicitly, as opposed to trusting them via certificate path validation to a trusted anchor or root certificate.

A subset of the S/MIME implementations that are currently available support the use of an implicit trust model using self-signed certificates. Self-signed certificates accompanying incoming signed messages from peers can be implicitly trusted and used to send encrypted messages to the peer entity. Other S/MIME implementations do not allow the use of self-signed certificates either for the local user or their peers. To allow rapid deployment of S/MIME in an environment where PKI path-based trust cannot be established, it is preferable to use S/MIME implementations that support an implicit trust model.

Single / Multiple Certificates for Local user. Some S/MIME applications have the capability to support multiple certificates for the local user. This allows the local user to belong to multiple PKI hierarchies simultaneously, selecting the certificate to use when interacting with a particular peer. For example, user A belong to infrastructures X and Y and has certificates K_x and K_y from infrastructures X and Y respectively. Entity B belongs to infrastructure X and can only validate certificates in X; entity C belongs to infrastructure Y and can only validate certificates within Y. When interacting with B, A selects certificate K_x. Likewise, A selects certificate K_y when interacting with C. Support for multiple certificates for the local user is thus a very desirable attribute in an S/MIME application.

Ability to Import PKCS #12 Credentials for Local user. PKCS (Public Key Cryptography Standards) #12 is a de-facto standard from RSA Laboratories for securely packaging credentials (public and private key pairs) for transport or storage [3]. Many S/MIME applications have built-in or companion modules that generate key pairs, and are able to dispatch certificate requests to Certification Authorities using the newly generated public key. In such cases, the ability to import PKCS#12 objects is not necessary. However, there are two situations where it becomes important for an S/MIME application to import PKCS#12 objects. In the first situation, a Certification Authority may perform key pair generation for every certificate issued by it; a PKCS#12 object is then sent back to the S/MIME user for import into the S/MIME application. In the second case, a key pair and certificate may be held within an external module (such as a browser,) and the user may be interested in importing the same set of credentials for use within the S/MIME application.

The ability of an S/MIME implementation to import and use PKCS#12 objects thus affects its interoperability with CAs and the ability to share digital credentials with other PKI-based applications.

Managing Peer Certificates.

Self-Signed Peer Certificate Support. The ability to support an implicit trust model using self-signed certificates from peers allows an S/MIME application to be fit for quick deployment in communities where a pervasive PKI is either lacking.

Acquiring Certificates for Peers. Peer certificates are acquired by S/MIME applications in any of the following three ways:

- Extracting certificates from incoming signed messages from peers
- Loading certificates from *.p7c files
- Lookup of peer certificates from a LDAP Repository

The lack of support for one or more of the above may hinder an S/MIME application from obtaining certificates for peer users, and therefore, from being able to communicate securely with them. For example, if an S/MIME client application only has the capability to extract certificates from signed messages, then it cannot interact with a peer S/MIME application that does not send certificates along with a signed message.

Support for Selective Trust of Peer Certificates. Occasionally, peer certificates that are acquired (through any of the mechanisms discussed in the last section) cannot be validated using any of the known trusted root keys embedded within the S/MIME application. In such cases, it is very useful if the S/MIME application provides the local user the ability to selectively trust peer certificates that have been acquired. Once the local user designates the peer certificate as trusted, secure, encrypted email can be sent to that peer.

Managing Root Certificates. Most S/MIME implementation comes preloaded with a set of root certificates, all or a subset of which may be designated as trusted. These trusted root certificates are used to validate the certificates of peers. This section describes some attributes that affect the management of root certificates.

Acquiring Certificates for Roots. Root certificates may be acquired via the same three ways (as mentioned in the last subsection) used to acquire peer certificates. Support for various means of acquiring root certificates for use within an S/MIME application allows it to use additional roots to establish trust in peer certificates. Conversely, lack of support for one or more of these ways, may disallow import of a particular root certificate, and prevent interoperability with a peer that is certified by that root authority.

Selectively Trusting Root Certificates. Having acquired or imported additional root certificates into an S/MIME application, it is very useful to have the ability to selectively trust one or all of the newly imported root certificates. Thus, if the local user is given the opportunity to designate newly imported roots as trusted, it may allow the local user to establish trust in all certificates issued by these additional trusted roots. Conversely, if additional trusted roots cannot be established within an S/MIME application, it may be impossible to communicate with a large set of potential peers.

3.2 Interaction with Certificate Authorities

S/MIME users need to obtain certificates signed by Certification Authorities (CA) to communicate securely with peers. The only exception is when self-signed certificates

are used within a small well-known community to establish implicit trust in peers. Most S/MIME applications have associated modules or software tools that allow the generation of a key pair on behalf of the local user, and the construction and dispatch of a certification request to a CA. The certificate request message is based upon the PKCS#10 format as specified in the S/MIME Version 2 specification.

Support for Multiple Mechanisms for Requesting Certificates from CAs. Certification Authorities or their delegates support one or more of the following transport mechanisms for incoming certification requests, and distribution of issued certificates:

- Web: The User's Web Browser connects to the CA's website to dispatch certification requests, or to collect an issued certificate.
- Email: The User sends an email to the CA's email address with the certification request. The CA may send an email back to the User with a reference to the location where the issued certificate may be picked up.
- In-Person/Floppy/Smart Card: The User places the certification request on a floppy or similar physical medium and transports it to the CA or its delegate. The CA or its delegate may return the issued certificate on a floppy or other medium (such as a smart card) for import and use by the User's application.

S/MIME applications that support all of the above mechanisms for interaction with a CA are able to request and receive certificates from the majority of CA products.

3.3 Interaction with Repositories

Certificate distribution in a small community may be achieved by users exchanging certificates with one another. However, the S/MIME Version 2 specification calls for the use of LDAP (Lightweight Directory Access Protocol) to interface with directories/repositories to obtain certificates and revocation information for users.

Publishing local user certificate. Typically, the CA that issues a certificate is responsible for publishing it in a repository. However, some S/MIME implementations also have the ability to publish the local user's certificate in a chosen directory. This feature is very useful in a domain where peers obtain each other's certificate from an organizational directory. Publication in the directory makes the user's certificate readily available to a large community of peers, and thus promotes interoperability.

Peer Certificate Lookup. When an S/MIME application supports the lookup of LDAP-based Directories for peer certificates, it gives the local user access to a large set of potential peer certificates, and the ability to interact with these peers.

3.4 Signing Outgoing Messages

This section describes various issues involved during signing of messages that may determine its level of interoperability.

Support for Opaque/Clear Signed Message Formats. S/MIME Version 2 provides for two data signing formats. In the "clear" or multipart format, the signature is separated from the signed data and is sent as an attachment. There is both an advantage and a disadvantage in using this signing format. The advantage is that the recipient can always read the message even if the recipient's e-mail application is not an S/MIME client and the signature cannot be verified. The disadvantage is that the message may undergo some format conversion as it transits a mail gateway that is not S/MIME- aware. This will cause the receiving S/MIME application to invalidate the signature.

This can be corrected by binding the signature with the message in a single binary file. The resulting format is labeled the "opaque" format. No conversion will be performed by a mail gateway on the binary file and the message can be verified by an S/MIME application that serves the recipient. However, because the message text is wrapped in a binary file, the recipient cannot read it if the recipient's e-mail application is not an S/MIME client.

The existence of two possible signing formats has led to some difficulties in S/MIME interoperability. Some applications sign in "clear" format, some sign in "opaque" format; others give the user a choice. The applications that support both formats for outgoing signed messages are guaranteed to be able to successfully interoperate with every other S/MIME application.

Support for Multiple Algorithms and Key Sizes. All currently available S/MIME implementations use RSA for signatures; the keys that are used vary between sizes 512/768/1024/2048. The hashing algorithm used within the signature could be SHA-1 or MD5. Some S/MIME applications support only a subset of the above algorithms for incoming signed messages. In order for two S/MIME implementations to exchange signed messages, they must support a common set of algorithms and key sizes. Thus the implementations that support both hash algorithms and various RSA moduli, and allow the local user to select the algorithms to use for specific outgoing signed messages enable the greatest level of interoperability with other S/MIME implementations.

3.5 Validating Incoming Signed Messages

Support for Opaque/Clear Signed Message Formats. Support for both signed message formats for validating incoming signed messages provides the highest level of interoperability with other S/MIME implementations that may support only one of the formats for outgoing signed messages. See similar subsection above for further details.

Support for Multiple Algorithm Choices and Key Sizes. Support for multiple hash algorithms and various moduli for the RSA signature keys for validating incoming signed messages promotes interoperability with a large number of sending clients. See similar subsection above for further details.

X.509v3 Certificate Path Validation. S/MIME Version 2 specifies the use of X.509v3 certificate path validation mechanisms for S/MIME implementations;

support for this type of path validation allows an S/MIME application to parse complex certificate chains to establish trust in peer certificates. All S/MIME applications that we have tested have the capacity to validate flat certification hierarchies, namely, the CA issues certificates to S/MIME users in a one level deep hierarchy. However, many implementations do not support the validation of certificates that are part of a multiple level hierarchy. In order to interoperate with the largest possible set of peers (some of which may send out signed messages with certificate chains that are part of a multiple level hierarchy), it is very useful if an S/MIME implementation supports fully compliant X.509v3 path validation.

3.6 Encrypting Outgoing Messages

In S/MIME, Version 2, an encrypted message is constructed as follows: a random symmetric key is used to encrypt the message, and the recipient's public key is used to wrap the symmetric key for key transfer purposes. On the recipient's side, the corresponding private key is used to unwrap the symmetric decryption key, and the latter is used to decrypt the message.

Support for Multiple Algorithm Choices and Key Sizes. The S/MIME Version 2 specification allows the use of various symmetric algorithms and key sizes for message encryption, and various RSA moduli for key exchange. Currently, S/MIME applications support one or more of the symmetric encryption algorithms, DES, Triple DES and RC2, with various key sizes. In order for an encrypted message to be passed between two S/MIME applications, both sides must support the same encryption algorithm and key size, and the same modulus for RSA key exchange. Some implementations support only a single algorithm and key size for encryption, or a single modulus for RSA keys. The implementations that support all or a large subset of the available algorithms provide the greatest level of interoperability with peer implementations with a limited set of algorithms.

3.7 Decrypting Incoming Messages

Selection of Local User Certificate for decryption. When the local user possesses more than one certificate, and receives an encrypted S/MIME message, the correct certificate and private key needs to be selected to decrypt the message. Some implementations leave the selection of the appropriate private key (from the set of available private keys) to the user. Others allow a transparent selection of the appropriate private key for decryption; this is very useful feature in environments where users routinely possess certificates from multiple public key infrastructures, and use them for communicating with peers from disparate trust domains.
Support for Multiple Algorithms and Key Sizes. See similar subsection above for details.

4 Usefulness of the Interoperability Characteristics

The characteristics and properties outlined in this paper provide us with a greater insight into the issues that affect the interoperability of a S/MIME implementation in a real-world scenario. Ideally, the S/MIME specification should be capable of addressing each of these issues and setting minimum requirements to allow a base level of interoperability between all compliant implementations. Understanding the intricacies of the various choices that can be made within the scope of the S/MIME Version 2 specification may help to fine tune the future S/MIME specifications.

Understanding the characteristics that affect interoperability also helps vendors of S/MIME products understand the implications of the implementation and design choices they make for their products. Knowledge of these characteristics is also important to the community of S/MIME product users and procurers. Users who are aware of their own environments with respect to the deployment of PKI products will be able to make an informed decision about which subset of the characteristics presented in this paper are relevant to their interoperability needs. Having defined their idealized profile for S/MIME products, they can then evaluate the available implementations from the various vendors and select the one that scores highest in the evaluation based upon their customized needs.

The characteristics described in this paper were derived through a study of the S/MIME specification and experimentation with S/MIME implementations. However, we believe that a large subset of these characteristics are also applicable to most other public key infrastructure based secure communication protocols, and their implementations. The lessons learned through the study of S/MIME should be easily transferable to other similar domains.

5 Analysis of the S/MIME Version 3 Specifications with Respect to the Interoperability Characteristics

S/MIME Version 3 uses the CMS instead of the PKCS#7 standard to build the S/MIME objects. CMS supports a set of signed attributes that are encapsulated within the signerInfo data type that is a part of each S/MIME signed object. CMS allows object identifiers (OIDs) for preferred algorithms to be conveyed using these signed attributes. However, there does not appear to be a way to support the conveyance of other critical information for the sender, such as signature format preferences, or trust anchors known to the sender, etc. Additionally, these capabilities seem to be supported only when a signed message is sent. When the enveloped data content type is used, only a limited set of originator information (certificates and CRLs only) may be included in the message – there does not appear to be a way for the originator to include their algorithmic preferences to their peers.

A deficiency that continues to exist in the Version 3 specification is that there is no mandate to support a particular signature format (opaque versus multipart). As we have noted in this paper, a number of the interoperability problems were related to the support of only one or the other signature formats in Version 2 products that we tested. It would be desirable to establish a baseline for the supported signature formats – this would allow a minimal level of interoperability between all S/MIME

implementations. Thus, we would recommend that the S/MIME specification be augmented to require that both sending as well as receiving agents MUST support the opaque signature format. In addition, sending and receiving agents SHOULD support the clear signing format to allow non-S/MIME capable mail agents to display the message contents.

A desirable feature of Version 3 specification is that it supports the ability to dynamically import additional trust anchors into an S/MIME product. Receiving agents MUST support the import of additional trusted roots and certificate chains from incoming S/MIME messages. During the import of additional trust anchors, receiving agents SHOULD allow the user to select whether or not to trust new root certificates that were imported. Other methods to allow import of additional trust anchors would also be desirable (for example, the import of self-signed .p7c files from a floppy).

6 Conclusions

In this paper, we have described a number of important properties that affect the ability of an S/MIME implementation to interoperate with its peer implementations. However, there are other issues that also affect the suitability of an implementation within a particular environment.

The usability characteristics of an implementation go a long way to promote the usage of the product. If secure email products provide daunting user interfaces, they will not be widely. One obvious recommendation to heightened user friendliness would be to transparently support the digital certificates of peers within the address book mechanisms provided by the basic email package. Thus, when a signed message comes in, the local user can add the sender to their local address book and thereby transparently add the sender's certificate to the address book entry. Conversely, when sending out encrypted email, the local address book could be used to select the receiver and transparently select the receiver's certificate (if present as part of the address book entry.)

Most current implementations also have little or no support for revocation checking of certificates. As public key infrastructures become widely deployed, the very real management problems such as certificate revocation need to be handled within the applications using the infrastructure.

In conclusion, we would like to point out that it is heartening to see the widespread adoption of the S/MIME secure electronic mail standard, and the availability of commercial products based upon the standard. Despite the fact that public key infrastructure technology is still in its infancy, and the standards are continuously evolving, the S/MIME vendors are making considerable progress in resolving the existing barriers to interoperability. In the near future, users will find that security services will be integrated into most e-mail applications.

7 References

[1] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998.
[2] Kaliski, B., "PKCS #10: Certification Request Syntax Version 1.5", RFC 2314, March 1998.
[3] Kaliski, B., "PKCS #12: Personal Information Exchange Syntax Standard, Version 1.0 Draft", 30 April 1997.
[4] Postel, J., "Simple Mail Transfer Protocol", RFC 821, Aug 1982.
[5] Crocker, D., "Standard for the format of ARPA Internet text messages", RFC 822, Aug-1982.
[6] Dusse, S., Hoffman, P., Ramsdell, B., Lundblade, L., and L. Repka, " S/MIME Version 2 Message Specification", RFC 2311, March 1998.
[7] Dusse, S., Hoffman, P., Ramsdell, B., and J. Weinstein, " S/MIME Version 2 Certificate Handling", RFC 2312, March 1998.
[8] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633.
[9] Ramsdell, B., "S/MIME Version 3 Certificate Handling", RFC 2632.
[10] Backman, D., "Secure E-Mail Clients: Not Quite Ready For S/MIME Prime Time. Stay Tuned", Network Computing Online, http://www.networkcomputing.com/902/902r22.html.
[11] Housley, R., "Cryptographic Message Syntax", RFC 2630.

8 Appendix

These are the products that were tested in order to derive the characteristics described in this paper:

- Baltimore Technologies MailSecure Exchange Plug-in Version 2.1
- WorldTalk WorldSecure Eudora Plug-in Version 3.05
- WorldTalk WorldSecure Exchange Plug-in Version 3.0
- Netscape Messenger Version 4.05
- Microsoft Outlook Express Version 5.0 Beta 2
- Microsoft Outlook 98

The DEDICA Project: The Solution to the Interoperability Problems between the X.509 and EDIFACT Public Key Infrastructures

Montse Rubia[1,2], Juan Carlos Cruellas[1], and Manel Medina[1]

[1] Telematics Applications Group - Department of Computer Architecture
Universitat Politècnica de Catalunya
c / Jordi Girona 1-3, Mòdul D6
08034 - Barcelona (SPAIN)
{montser, cruellas, medina}@ac.upc.es

[2] Safelayer Secure Communications S.A.
Edificio World Trade Center (s4)
Moll de Barcelona s/n
08039 – Barcelona (SPAIN)
montse@safelayer.com

Abstract. This paper introduces the barriers of interoperability that exist between the X.509 and EDIFACT Public Key Infrastructures (PKI), and proposes a solution to remove them. The solution goes through the DEDICA[1] (Directory based EDI Certificate Access and management) Project. The main objective of this project is to define and to provide the means to make these two infrastructures inter-operable without increasing the amount of information to be managed by them. The proposed solution is a gateway tool interconnecting both PKIs. The main goal of this gateway is to act as a TTP that "translates" certificates issued by one PKI to the other's format, and then signs the translation to make it a new certificate. The gateway will, in fact, act as a proxy Certification Authority (CA) of the CAs of the other PKI, and will take the responsibility of the certified data authenticity, on the behalf of the original CA.

1. Introduction

The security services based on asymmetric cryptography require a Public Key Infrastructure (PKI) to make the public key values available.

Several initiatives around the world have caused the emergence of PKIs based on X.509 certificates, such as SET (Secure Electronic Transaction) or PKIX (Internet Public Key Infrastructure). Another PKI type is the one based on the EDIFACT certificate. These infrastructures are not interoperable, mainly due to the fact that the certificates and messages are coded in different way (ASN.1 and DER are used for X.509 PKI, whilst EDIFACT syntax is used for EDIFACT PKI).

[1] This project has been funded by the EU Telematics program and the Spanish CICYT, and has been selected as one of the pilot projects to promote the telematic applications by the SMEs by the G7.

R. Baumgart (Ed.): CQRE'99, LNCS 1740, pp. 242–250, 1999.

DEDICA (Directory based EDI Certificate Access and management) is a research and development project. Its main objective is to define and to provide means to make the two above-mentioned infrastructures inter-operable without increasing the amount of information to be managed by them. The proposed solution involves the design and implementation of a gateway tool interconnecting both PKIs: the certification infrastructure, based on standards produced in the open systems world, and the existing EDI applications, which follow the UN/EDIFACT standards for certification and electronic signature mechanisms.

The main goal of the gateway proposed by DEDICA is to act as a Trusted Third Party (TTP) that “translates” certificates issued in one PKI to the other’s format, and then signs the translation to make it a new certificate: a derived certificate. In this way, any user certified, for instance, within an X.509 PKI could get an EDIFACT certificate from this gateway without having to register in an EDIFACT authority, saving not only time and money, but also allowing the users to use the same private key for both environments. The gateway will act, in fact, as a proxy Certification Authority (CA) of the CAs of the other PKI.

The figure 1 shows the DEDICA gateway context. Each user is registered in his PKI and accesses the certification objects repository related to its PKI. The DEDICA gateway must be able to interact with the users of both PKIs in order to serve requests from any of them. It must also be able to access the security object stores of both PKIs, and to be certified as EDIFACT and X.509 CAs.

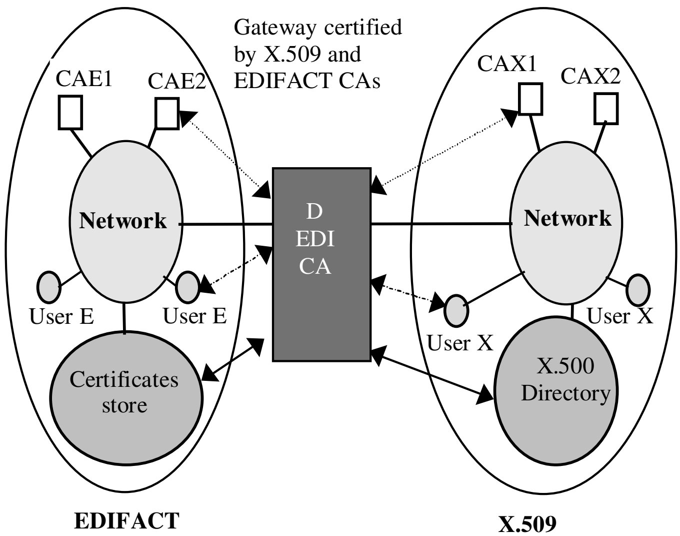


Fig. 1. DEDICA gateway context.

2. Functionality of the gateway

The interoperability problem between the X.509 and EDIFACT PKIs was focused by the DEDICA project in two levels: .

1. The different formats of the certificates: The DEDICA consortium, after an in-depth study of the contents of both types of certificates, specified a set of mapping rules that makes possible the two-way translation of both types of certificates.
2. The different messages interchanged by the entities of the PKIs: whereas in the EDIFACT world the UN/EDIFACT KEYMAN message is used to provide certification services, in the X.509 world a set of messages specified for each PKI (PKIX on the Internet, for instance) are used.

The DEDICA gateway assumes the role of a TTP for users of both infrastructures. The gateway accomplishes a process of certificate translation from EDIFACT to X.509 and conversely; however **this translation process is not strictly a mapping at level of certificate formats, since the gateway adds a digital signature to the** mapped data. In addition to that, in some cases, it is not possible just to move data from one certificate to the other, due to format restrictions (size, encoding). In these cases the gateway has to generate tagged data for the derived certificate, that will allow it to reproduce the original data, kept in internal records (e.g. names mapping table, see fig. 3). When the X.509 certificate has private extensions, the gateway will just ignore them, since they are assumed relevant only to other applications.

Full details of the mapping mechanism between both infrastructures may be found at: http://www.ac.upc.es/DEDICA/ and at DEDICA CEC-Deliverable WP03.DST3: *Final Specifications of CertMap Conversion Rules* [5]. The DEDICA gateway is able to offer a basic set of certificate management services to users of different infrastructures:

1. Request of an EDIFACT certificate from an X.509 certificate generated by an X.509 CA.
2. Verification of an EDIFACT certificate generated by the DEDICA gateway (coming from the mapping of an X.509 certificate).
3. Request of an X.509 certificate from an EDIFACT certificate generated by an EDIFACT CA.
4. Verification of an X.509 certificate generated by the DEDICA gateway (coming from the mapping of an EDIFACT certificate).
   The above requests will be carried out making use of the appropriate messages from the infrastructure: KEYMAN PACKAGES for EDIFACT, and PKIX for X.509.

2.1. Request of a derived certificate

In the scenario shown in Figure 2, an X.509 user (user X) that may want to send EDIFACT messages to an EDIFACT user (user E) using digital signatures or any security mechanism that involves the management of certificates. This user needs a certificate from the other Public Key Infrastructure (in this case, the EDIFACT PKI). He then sends an interchange to the gateway requesting the production of an EDIFACT certificate “equivalent” to its provided X.509 one. This interchange will

contain a KEYMAN message (indicating a request for an EDIFACT certificate) and the X.509 certificate of this user in an EDIFACT package (EDIFACT structure capable of containing binary information).

The gateway will validate the X.509 certificate. If the certificate is valid (the signature is correct, it has not been revoked, and it has not expired), it will perform the mapping process, and will generate the new EDIFACT certificate. After that the gateway will send it to user X within a KEYMAN message.

Now user X can establish a communication with user E using security mechanisms that involve the use of electronic certificates through the new EDIFACT certificate, sending him an EDIFACT interchange with this certificate.

2.2. Validation of a derived certificate

Following the process described in the previous section, user E, after receiving the interchange sent by user X, requests validation of the certificate generated by the DEDICA gateway by sending the corresponding KEYMAN message to the gateway.

The gateway determines whether the EDIFACT certificate has been generated by itself, and proceeds with the validation of the original X.509 certificate, to find out whether it has been revoked or not, and of the derived EDIFACT certificate. The EDIFACT user could only check the derived certificate, since it has no access to the original environment. The general process of validation of derived certificates is as follows:

1. It verifies the validity of the derived certificate. This requires checking of:
   (a)The correctness of signature, using the public key of the gateway.
   (b) Whether the certificate can be used in view of the validity period.
2. The gateway accesses to the X.500 Distributed Directory, in order to get the original X.509 certificate and the necessary Certificate Revocation Lists (CRL).
3. It verifies the signature of the original certificate, and checks the validity period.
4. The gateway verifies the certification path related to the original X.509 certificate, and checks that its certificates have not been revoked.

Now the DEDICA gateway will send the positive or negative validation response to the EDIFACT user within a KEYMAN message.

3. Gateway architecture

The DEDICA gateway has two main architectural blocks: the **CertMap** and the **MangMap** modules.

3.1. CertMap module

The CertMap module is responsible for performing the certificate translations following the mapping rules specified by the DEDICA consortium in Deliverables WP03.DST3 ([5]).

The CertMap is composed of three main modules: the CM_Kernel module, the EDIFACT certificate coding/decoding module, and the set of APIs needed to allow

the CM_KE to interact with external software tools (the ASN.1 API and the Cryptographic API).

The **CM_Kernel** module (**CM_KE**) coordinates the operations performed by all the other CertMap modules. Four groups of information presents in both certificates have been identified: Names, Algorithms, Time and Keys. For each one of these groups, inside the CM_Kernel, a software module implements the appropriate relevant translation process: the CM_Names, the CM_Algorithm, the CM_Time and the CM_Keys modules.

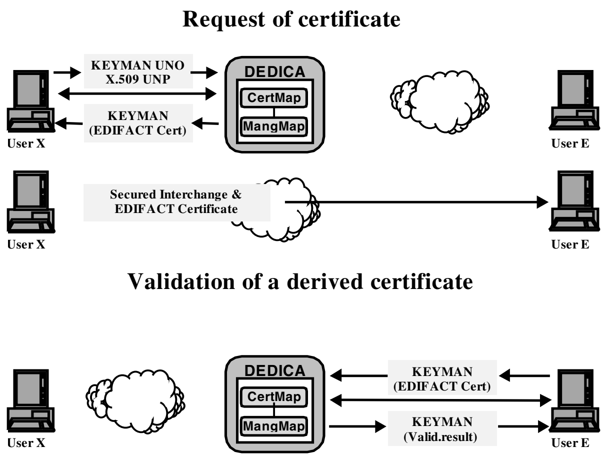


Fig. 2. Functionality of the DEDICA gateway

Mapping between X.509 and EDIFACT certificates. The Certificate Mapping Rules developed in DEDICA were designed in such a way that the translated information was relayed as precisely as possible from the original certificate to the derived one. A number of issues had to be taken into account:

- **Specification syntax and transfer syntax** for the transmission. The EDIFACT certificates are specified following the EDIFACT syntax, and they are transmitted coded in printable characters. However, in the X.509 environment the ASN.1 Abstract Syntax and the DER rules are used.
- **Naming System**. In the X.509 world, the basic mechanism of identification is the DN (Distinguished Name) [6], which is associated with an entry in the DIT (Directory Information Tree) of the X.500 Distributed Directory. On the other hand, the EDIFACT certificate supports both codes (i.e., identifiers assigned by authorities) and EDI party names. The DEDICA gateway performs a name mapping between the DNs and the EDI Names, according to guidelines defined in EDIRA (EDIRA Memorandum of Understanding) [7]. EDIRA proposes an identification mechanism compatible with the DN strategy in X.500. The DEDICA Deliverable WP03.DST2([4]) contains the specifications of the conversion rules that are used by the CertMap module to execute the mapping between DNs and EDI Names.

- **Extension mechanism**. Version 3 of the X.509 certificate has an extension mechanism that allows it to extend the semantics of the information that it carries out. However, at present the EDIFACT certificate does not have any extension mechanism, and its syntax specification does not allow to specify such a wide variety of information. In the mapping of X.509 certificates version 3, only the following extensions will be mapped: *keyUsage* and *subjectAltName*. Other extensions, mainly the private ones, even if they are tagged as critical for the intended applications of the original certificate, are ignored, since we assumed that user and issuer know and accept the EDIFACT certificate format, when they make the application for a derived certificate.
- **Digital signature**. When the gateway finishes the mapping process, it automatically generates a new digital signature. In the certificate field identifying the issuer entity, the DEDICA gateway identifier will appear, instead of the original certificate issuer identification.

The figure 3 shows the internal structure of the CertMap module. It also shows the sequence of operations that will take place inside the CertMap to generate an EDIFACT certificate from the initial X.509 one.

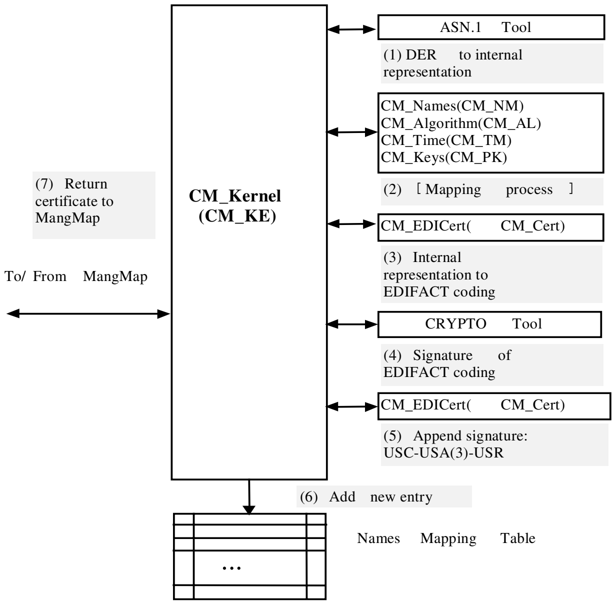


Fig. 3. Mapping process from X.509 to EDIFACT

3.2. MangMap module

The MangMap module of the DEDICA gateway converts certain operations of the KEYMAN message into equivalent operations (messages) in the X.509 PKI (including X.500 access).

MangMap is also the general management module for DEDICA gateway. It receives all the requests sent to it and chooses which information has to be recovered from external repositories, what type of translation is needed, and what results must be generated and sent to the requesting entity.

Internal structure of the MangMap module. The main blocks of the MangMap are shown in Figure 4, and its functionality may be summarised as follows:

- **MangMap Kernel (MK) module**
  The Kernel module of the MangMap controls all the actions within the DEDICA gateway and co-ordinates the co-operation between the different DEDICA modules.
- **KEYMAN Handling (KH) module**
  On reception of KEYMAN messages from an end user, it checks the protection applied to the KEYMAN, analyses it, interprets the message and converts it into an internal request to the MangMap Kernel block. On reception of requests from the MangMap Kernel block, it builds KEYMAN messages, applies the required protection and makes the KEYMAN available to the communication services.
- **X.509 Public Key Infrastructure Messages Handling (XH) module**
  On reception of relevant X.509 public key infrastructure messages from an end user, XH module checks the protection applied to the message, analyses it and converts the message into an internal request to the MK.

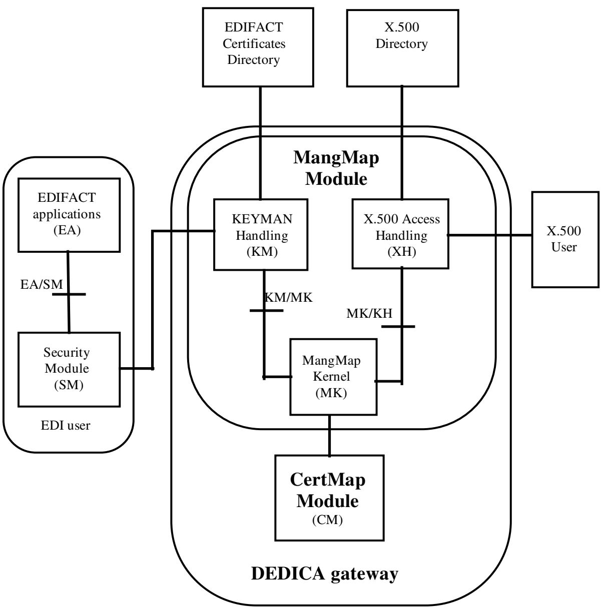


Fig. 4. Structure of the DEDICA gateway

XH is also able to access the X.500 Directory in order to get X.509 certificates, revocation lists and certification paths. XH will be able to send requests to X.500 and to obtain and interpret answers from it. Due to the complexity of DAP, the XH module uses the LDAP (Lightweight Directory Access Protocol) [8] interface to access the X.500 Directory. LDAP offers all the functionality needed to interact with the X.500 Directory at much lower cost.

On reception of requests from MK, it builds relevant X.509 public key infrastructure messages, applies the required protection and makes the messages available to the communication service.

4. Conclusions

This work has proved the suitability to launch a TTP service to translate security objects between different protocol environments. The problems found in this project are of general nature, and the solutions adopted here may be extrapolated to any other pair of environments.

Other arising PKI services, like SPKI or UMTS (Universal Mobile Telephone System), or XML-EDI are potential candidates to use the results of this work. But it will be possible to extend the results of this work to other TTP services, like Time Stamping, Attribute certification, etc.

The data type conversion based on translation table may solve any format incompatibility, and the message mapping strategy used to handle the different certificate management strategies may also overcome with almost any mismatching services between the two protocols being linked.

As far as both, environments and protocols, have the same goals, the details of data and service elements not having a corresponding element on the other environment may either:

a) be just overridden because it is not useful in the destination application, or
b) be replaced by an equivalent data or service element with similar meaning in the destination protocol.

The interoperability between the X.509 and EDIFACT PKIs can be greatly enhanced by facilities such as the DEDICA gateway, which acts as a TTP capable of offering a basic set of certificate management services to users of both infrastructures.

The DEDICA project has set up a gateway to translate the security objects between X.509 and EDIFACT. This solution also provides interoperability between EDIFACT and all the other tools used in electronic commerce, since all of them authenticate the entities using X.509 certificates.

The DEDICA gateway is being integrated in several pilot schemes and projects in the context of electronic certification, such as the TEDIC system, the AECOC-UPC EDI over Internet project, or in the SAFELAYER[2] X.509 Certification Authority.

The DEDICA service is interesting to both the large enterprises and SMEs, although this gateway is mostly interesting to SMEs. This is because it allows them to use security in the interchange of messages, without the need to pay registration fees

[2] Safelayer Secure Communications S.A. is a company provider of PKI and SET software solutions <http://www.safelayer.com>

in several infrastructures. This was the reason for which DEDICA was selected as one of the G7 pilots projects to promote the use of information technology by the SMEs.

The main advantage for the user will be to share the authentication mechanism (digital signature, tools, etc.) between the various applications where they can be applied, avoiding the burden of having to register with various services in order to satisfy one single user requirement.

Moreover, the service has been quickly deployed and made available, thanks to the fact that no additional registration infrastructure is needed, due to its compatibility with the EDIFACT and X.509 infrastructures. This service will promote the use of Internet by EDI applications (since it will allow them to secure the interchanges which has been identified) in spite of the major barriers to the deployment of EDI over Internet in the past.

Within the project, several pilot schemes have been launched to demonstrate the system in the following fields: customs, electronic chambers of commerce, tourism, electronic products manufacturers, EDI software providers and electronic payment in banking and public administration.

References

1. Security Joint Working Group, Proposed Draft of a MIG Handbook UN/EDIFACT Message KEYMAN, 30. June 1995.
2. Security Joint Working Group: Committee Draft UN/EDIFACT CD 9735-5, Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules, Part 5: Security Rules for Batch EDI (Authenticity: Integrity and Non-Repudiation of Origin, Release 1, 14. December 1995.
3. DEDICA Consortium, CEC Deliverable WP03.DST1: Technical description of X.509 and UN/EDIFACT certificates, July 1996.
4. DEDICA Consortium, CEC Deliverable WP03.DST2: Naming Conversion Rules Specifications Requirements, July 1996.
5. DEDICA Consortium, CEC Deliverable WP03.DST3: Final Specifications of CertMap Conversion Rules, July 1996.
6. Network Working Group, RFC 1779: *A String Representation of Distinguished Names*, ISODE Consortium, 1995.
7. EDIRA - Memorandum of Understanding for the Operation of EDI Registration Authorities, Final Draft. November, 1993.
8. Network Working Group, RFC 1959: *An LDAP URL Format*, 1996.
9. PKIX Working Group, INTERNET-DRAFT: *Internet Public Key Infrastructure, X.509 Certificate and CRL Profile*, 1997.
10. Fritz Bauspieß, Juan Carlos Cruellas, Montse Rubia, *DEDICA Directory based EDI Certificate Access and Management*, Digital Signature Conference, July 1996.
11. Juan Carlos Cruellas, Damián Rodriguez, Montse Rubia, Manel Medina, Isabel Gallego, WP07.DST2. *Final Specification of MangMap Conversion Rules*, DEDICA Project, 1996.
12. Juan Carlos Cruellas, Damián Rodriguez, Montse Rubia, Manel Medina, Isabel Gallego, WP07.DST1. *Final Specifications of MangMap*, DEDICA Project, 1996.

r r c
r r r c I c

a l a - illo , ar a - ila , a d a o al - ar os

U e a P ec ca e a T S Te ec cac
D Tec g a ca
a U e a a 8 4 a S a
{reillo, agonmar}@tfo.upm.es
U e a P ec ca e a T S Te ec cac
D a e a ca ca a
a U e a a 8 4 a S a
csa@mat.upm.es

c The a h e c be he e he ffe e b e c ech e a e a ha ge e The e ech e e e e ffe e ce g a g h ach e g g e f ffe e ec e e h e a e a h gh c a e h gh e ab ech e ha ge e c h gh acce e a e e h gh ec a e ech e ha e bee e f c ea g ha ge e e ab h e e ce g a g h ch a e c ea ab fi e ha e bee e ec ea e he c a a c e a e ec g The a ge f a a g he e b e c ech e f a e be e e c e h he e g f e e c S e he e he e e a e e a ab e age e a Th e a ca a be e e e e e b e f a ch a h hea h ec a e acce c a e e g e a he ea g f h a a e he b e c e fica ha bee e f e The e a ch e ha bee a a ca a a e e e e e ab he b e c e fica ha h be e f e e he a ca e be ab e e ac he e e a e f he ca

I r c

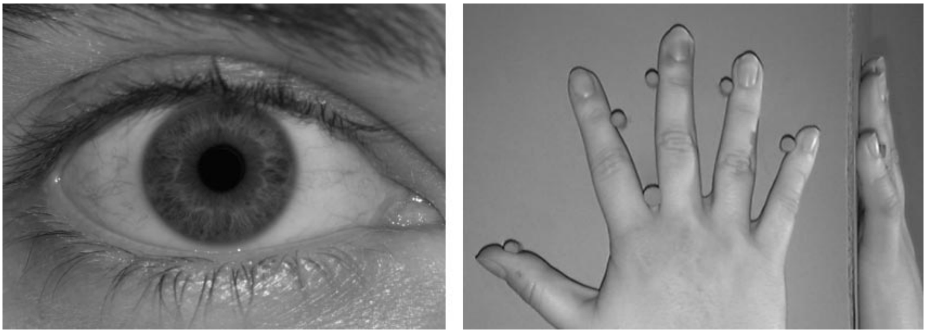
o ada s, o of t ai t r ats t at I s st s a d s rit iro ts a a , is t possibilit of a i g i tr d rs i t s st . is is or all sol d b s r a t ti atio s s bas d o pass ords, s r t od s a d/or id ti atio ards or to s. s bas d o l o pass ords or s r t od s a b ra d b i t r pti g t pr s tatio of s a pass ord, or b o t rf iti g it (ia pass ords di tio ari s or, i so s st s, ia br tal for atta s). t ot r a d, a i tr d r a atta s st s bas d o id ti atio ard or to s b robbi g, op i g or si lati g t at ard or to . If t s s d i t s st is bas d bot o a ard a d a pass ord (s all all d rso al Id ti atio b r - I), t i tr d r s o ld appl

. au gar (d.): ' , 7 , pp. – , .
◯ pr g r- r ag r d rg

or ffort to gai tr to t s st , a d it or ad a d t ologi s, s as s art ards, so l rabiliti s of t s st o ld b a oid d (.g. br tal for atta s ar i possibl d r a ll-d d s art ard).

t it t ost ad a d t iq s, a t ti atio s s bas d o pass ords a d id ti atio ards a a l gal li itatio : a p rso a ot b l gall id ti d b t o l dg or poss ssio of so t i g, b t o l b t as r of so biologi al b a io ral f at r s. is r q isit is o l sol- d b bio tri t iq s s as sp a r ri atio , sig at r r og itio or as r t of g rpri t, iris patt r or a d g o tr . a bio tri t iq as its o ad a tag s a d disad a tag s. il so of t pro- id or s rit , i. . lo r als pta at ( ) a d als j tio at ( ), ot r t iq s ar ap r or b tt r a pt d b al s rs.

a t ors r port r a bio tri & proj t r t o bio tri t - iq s a b a al s d a d d lop d: iris patt r a d a d g o tr . Iris att r og itio as os for pro idi g a tr l ig r liabilit bio- tri id ti atio . Its r liabilit is o l i pro d b ti al a i g i is ig l r j t d b al s rs for si g las r s a i g i sid t . ai disad a tag of t is t iq is o l its ig ost, ot o l o o i al b t also o p tatio al. t ot r a d, Ha d o tr as r t as o- s as a di / ig s rit t iq it a di q ip t ost, lo o p tatio al ost a d r lo t plat si . ft r t is i trod tio , a bri f pla atio of bot s st s (rst iris patt r , follo d b a d g o tr) ill b gi . ai r s lts a i d it bot t iq s ill b s o , di g t is or it t al o l sio s obtai d.



Sa e f he ef a ha he gh bef e e ce g a fea e e ac

Ir r c

ro all bio tri t iq s o toda , iris r og itio is o sid r d to b t ost pro isi g of all for ig s rit iro ts. is t iq pr s ts

s ral ad a tag s o par d to ot r t iq s, it o l o ai disad a - tag : t ost. t o sid ri g t o rall osts t at s ppos t i stallatio of a ig s rit s st , t is disad a tag o ld b i i i d.

Iris r og itio is bas d o t ara t ri atio of t patt r of t iris. di al a d for si st di s a pro t at a iris as ig r i it t a ot r t iq s, i. . t probabilit of di g t o iris patt r s id ti al is arl ll (id ti al t i s do ot a t sa iris patt r a d t t o s of t sa p rso a diff r t patt r s). ot r stro g ara t risti of t is t iq is t stabilit of t patt r . ft r t adol s t patt r as o pl t l ol d a d t prot tio of t or a a s a odi atio i t patt r i possibl , l ss a ajor i j r d stro s part of t a d, of o rs , t isio of t s r. iologi al st di s a affir d t at t iris patt r is ot i fl d b ag , a d o o isio ill ss as opia or atara t do ot aff t iris s i a s s . ll t i it of t is t iq l ads to a als pta at ( ) arl ll, il its stabilit allo s to r a r all lo als j tio at s ( ).

Iris r og itio s st s do ot s ff r fro ig s r r j tio d to t s of id o or p otograp a ras, i st ad of las r b a s s as t o s s d for r ti al s a i g i l ads to o sid r t latt r t iq so o i asi . o t rf iti g a iris is arl i possibl l ss a ol s rg r is ad i t it t t r at of losi g t isio i t at . s of o ta t l s s it a op of ot r s r's patt r pri t d o it is asil d t t d b a s of t o ti o s i ol tar o t of t iris, i is ot pr s t i a pri t d o .

. r pr c ss r r c r c

s t rst pro ss, t iris lo atio a d isolatio is p rfor d. is is p rfor d ta i g pro t fro t ir lar patt r of t iris it i t st d i g t rst d ri at of t i t sit of t i ag aro d a ir l it d tr a d ariabl radi s s

$$\frac{\partial}{\partial r} \oint_{x \ ,y \ ,r} \frac{I(x,y)}{2\pi r} \, ds \ . \qquad (\ )$$

sa pro ss is p rfor d to li i at t p pil fro t iris. isolat d, t r s lti g i ag is str t d for b tt r pro ssi g. a l t ltir sol tio a al sis is arri d o t. ral ltir sol tio algorit s a b st di d (.g. [2], [ ] a d [6]) a i i g b st r s lts it r al s tri abor lt ri g

$$G(x,y) = exp\left\{-\frac{}{2}\left(\frac{(x \ \ os\theta + y \, si \ \ \theta)}{\delta_x} + \frac{(x \, si \ \ \theta - y \ \ os\theta)}{\delta_y}\right)\right\}$$

$$\ os(2\pi\omega(x \ \ os\theta + y \, si \ \ \theta)). \qquad (2)$$

ft r obtai i g t a l t o ffi i ts, a r d d s t of t as b s l - t d t ro g pri ipal o po t a al sis. it t s t of data os , a pri ar patt r is for d. is patt r is s d i t r statisti al d isio s s for t ri atio pro ss: lid a a d Ha i g dista s a d a ssia i - t r od lli g ( ) [7]. I t is appli atio , dista s b t a t ti s a d i post rs ar so diff r t (aro d . for a t ti s a d . for i post rs), t at a i rsal t r s old o ld b appli d, b i g s ffi i t t sag of - lid a a d Ha i g dista s i st ad of s, it t ad a tag of lo r o p tatio al ost of t for r t o o par d it t latt r.

r r

i porta of a d g o tr as a bio tri t iq r li s o its - di /lo ost a d o its gr at a pta b t s r bas d o t follo i g t r ai poi ts: it as ot a poli i pli atio (.g. g rpri t ri atio is los l r lat d to poli for ost of t s rs), t s st is r all as to s (ot li sp a r ri atio it o t b i g t ro g a t l p o or iris r o- g itio) a d it do s ot i pl p si al i asio s of s r's ital orga s (s as s i r ti al s a i g). s it ill b s o , t r ar ot r fa ts t at a a d g o tr a opti al sol tio for so s rit iro ts, s as t t plat si i is t lo st of all t bio tri t iq s isti g toda .

t t ai disad a tag of t is t iq is t "la " of s rit . o - par d to o o l o sid r d ig s rit t ods (li g rpri t, iris a d r ti al s a i g), a d g o tr a d g r s ar ig r, d to t lo r i it a d stabilit of t a d t plat o par d it t abo - tio d t iq s. i it a d stabilit ar t o ara t risti s of a bio - tri t iq t at a b st di d s parat l . a s of t lo i it of t g o tr of t a d (i. . t possibilit of di g t o a ds id ti al), t is t iq is ot r o d d for ig s rit iro ts, b t t l l of s rit it gi s, a s t is t iq alid for di s rit a ss o trol s st s or s. lo stabilit of t a d g o tr is a probl t at a b sol d i t o a s: b p rfor i g r lati as r s a d/or b adapti g t t plat a ti t s r is a t ti at d b t s st .

3. p r r pr c ss r c r c

s i a bio tri s st t rst st p is t sig al apt r . I a d g o tr a digital a ra is s d for t is tas . i ag apt r d s o s ot o l t r rs of t pal b t also t lat ral i of t a d i ill s r as a ig ti g fa tor for t f at r s tra t d. p oto ill b ta t a d is orr tl pla d i t s st , as it ill b i di at d b positio a d pr ss r s sors.

ppl i g gradi t as t t iq s, t dg of t a d is q i l obtai d, a d r ad to p rfor t f at r tra tio . ral para t rs r as r d, fro t idt of t pal a d g rs, to t l gt a d ig t of t latt r.

a gl s for d i t p ala g joi ts r also ta i to a o t. pri ipal o po t a al sis as b do to s l t t para t rs t at ill b s d i t s r's t plat . bsol t as r s, as ll as r latio s b t t a ta part i t a al sis. orr tio s a b ad a ordi g to t pr ss r do b t s r. a al sis s o d t at it a lo b r of para t rs, s as of t , satisfa tor g r s for a d a b obtai d. I r asi g t b r of para t rs, a d data o ld b d r as d. it prop r para t r odi atio , t t plat si o ld b fro 9 to 2 b t s, i a s t is t iq id al for i i i i g t plat storag a d lo ri g o p tatio al ost of t ri atio pro ss.

ft r a al si g diff r t ri atio t ods, fro t o s bas d i tri s (.g. Ha i g a d lid a dista s), to t o s bas d o t statisti al d isio t or (.g. a ssia i t r od lli g), a d o sid ri g t ral t or approa it a d radial basis f tio s, t r s lts obtai d s o t at t t od it t b st rat b t o p tatio al ost a d + is t Ha i g dista , alt o g for b st r liabilit s ar r o d d (as s i t t s tio).

3. I pr

it t s st d lop d as plai d abo , o rall rror rat is b lo %. r latio b t , a d t is rat o ld b odi d (as said) pla - i g it t t r s old al , d p di g o t sp i ds of t s st . t t stabilit li itatio s t at t is t iq as, ar s o t is s st is s d o r a lo g p riod of ti . d lt s rs gai i g or losi g ig t a a g absol t as r s, a d if t ig t diff r is larg o g , a a g a app ar i t r lati as r s. t ot r a d, o -ad lt s rs (i. . s rs i t ir gro i g ars), a g o ti o sl t ir as r s. lt o g t latt r as is ot i porta t i ost iro ts, t i pro t r port d b t a t ors also sol s it. is i pro t is alidat d bas d o t o pot - s s:

s s gai i g or losi g of ig t or ig t, i ol o og o s a g s i a d g o tri as r s, a gi g absol t as r s b t ot t r lati o s.

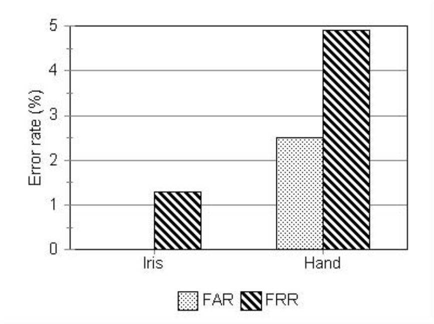
s s sp d of a gi g t a d f at r s, is slo o g to o sid r t at o i porta t ariatio ill o r i a p riod of o .

rst pot sis sol s ost of t probl s b ta i g r lati as r s i st ad of absol t o s. a s to t s o d pot sis, stro g r prot tio a b i l d d i t bio tri t plat s t ro g adaptatio . is adaptatio s o ld o sid r ot t a g i a si gl att pt, b t t ol tio of a s t of t . or a pl , t last s ssf ll r og i d att pts o ld b a rag d it t t plat , aft r si g a ig ti g fa tor for a of t s

as r ts, i d p d o t p riod of ti a o g t . it t s i -pro ts, t stabilit of t f at r s is i r as d a d t r for , g r s r ai t sa t ro g o t ti .
it t is a rag pro ss, i fl of a pot tial i tr d r ro gl r og i- d as t s r a t ti at d, is r d d. If t s st is bas d o t storag of t t plat s i a s r's s art ard, i st ad of i a tral databas , t t r at is d r as d or , a d b a s t is t iq s s a r s all t plat , o or li itatio s ist a d t a rag o ld b p rfor d it t last t or t t s ssf l att pts. rt r or , t at ati al op ratio s i ol d i t ol pro ss ar si pl o g to abl pro ssi g ti s b lo t o s d d for ot r t iq s a d it l ss po rf l i ropro ssors (.g. si g -bit pro ssors).

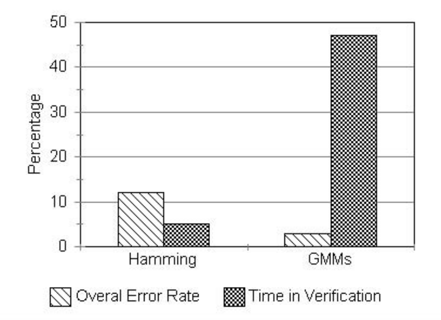
4 c

ft r d sig i g a d d lopi g t bio tri s st s plai d abo , t ai r s lts obtai d a b as p t d, it ll for iris patt r r og itio a d lo r t a t o obtai d for a d g o tr (s ig. 2). Ho r, iris f at r tra tio s o ld b i pro d to lo r t it o t i r asi g t o p tatio al ost.

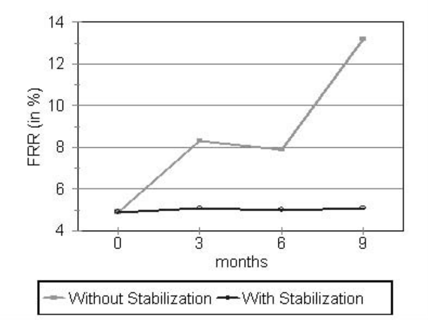


R a RR f a e ec g a ha ge e ea e e

t ot r a d, t r s lts obtai d it a d g o tr as r ts ar r satisfa tor , b i g abl to a i o rall rror rat s b lo % it a bas d ri atio algorit . If o p tatio al ost is a ig r stri tio , Ha i g dista s a a a alt r ati it t sa ri of i r asi g t o rall rror rat p to 2%, as it a b s i t t ill stratio .
i all t p rfor a of t a d bio tri s st as b a al s d t ro g o t 9 o t s, it a d it o t t stabili atio i pro t, s o i g a i r as of t o adaptatio is pr s t a d absol t as r -ts ar s d, il it t stabili atio t o rall rror rat as b pt i si ilar g r s.



e a e a e a e c e e fica f he h e ce e ha ge e b e c e h a g a ba e e fica a g h



S ab e e ha ge e b e c e

it t r s lts obtai d, bot t iq s a b i pl t d i s all b dd d s st s, s as a s art ard. ri atio rat s obtai d ar satisfa tor for ost of t appli atio s si ar l ss t a %, alt o g for ig s rit iro ts iris r og itio is r o d d.

r c

e e c c f he e Pa ebe c 4
Da g a gh fi e ce a Rec g f Pe b a Te f
S a ca e e e ce T a P 5 48

D a R a P Pa e a fica a Sce e a h e
& S
4 a a e a f D g a age P ce g P e ce a 8
5 a e R Pa a S e c Pe a e fica e e
S c e e ca e c P b he
a a c U a a h ee S T S e ge e c
Tech e ge a ace Rec g R P e

Re D R e R R b Te e e e S ea e e fica U g a a e S ea e e T a S eech a P ce g 5 8

8 Sa che Re R a e a c cce S e h a e e e fica a S a a P cee g f he ST fe e ce be b he c be

Scha ff R D g a age P ce g a e h e & S 8

Sch¨ a Pa e a fica fie e f a ca a e a a ache h e & S c

Z e a S a a ech e c 4

Author Index

CQRE [Secure]

November 30 - December 2, 1999, Düsseldorf, Germany

Program Chair

Rainer Baumgart, Secunet, Germany

Program Committee

Johannes Buchmann .... University of Technology Darmstadt, Germany
Dirk Fox ....Secorvo, Germany
Walter Fumy.. Siemens, Germany
Rüdiger Grimm... GMD, Germany
Helena Handschuh...Gemplus / ENS, France
Pil Joong Lee .... Postech, South Korea
Alfred Menezes .... University of Waterloo / Certicom, Canada
David Naccache... Gemplus, France
Clifford Neumann... University of Southern California, USA
Joachim Posegga ....Deutsche Telekom, Germany
Mike Reiter.. Bell Labs, USA
Matt Robshaw.. RSA Labs, USA
Richard Schlechter...European Commission, Belgium
Bruce Schneier .... Counterpane, USA
Tsuyoshi Takagi ....NTT, Germany
Yiannis Tsiounis...Spendcash, USA
Michael Waidner ....IBM, Switzerland
Moti Yung .... CertCo, USA
Robert Zuccerato ....Entrust Technologies, Canada

Your gateway to
IT-Security
Managing
the e-business
revolution
CQRE
SECURE
NETWORKING
EXHIBITION
& CONGRESS
DÜSSELDORF
8.-10.11.2000
Important dates:
deadline for submission of papers .... May 25,2000
deadline for submission of proposals .... June 1, 2000
notification of acceptance ....July 28, 2000
deadline for submission of complete papers .... August 20, 2000
www.cqre.net
Media partner of CQRE [Secure]:
Wirtschafts
Woche
Registration:
Alexandra Beck
CCD.
Congress Center Düsseldorf
Tel. +49(0)211/45 60-84 08
Fax +49(0)211/45 60-85 56
email: BeckA@ccd.de
Messe Düsseldorf GmbH
Postfach 10 10 06
D-40001 Düsseldorf
Germany
Tel. +49(0)211/45 60-01
Fax +49(0)211/45 60-6 68
www.messe-duesseldorf.de
Messe
Düsseldorf